Seqrite Unified Threat Management 2.2

Release Notes

Dated Feb 20, 2019

Seqrite Unified Threat Management

www.seqrite.com

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Unified Threat Management is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

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**
UTM2.2	20 Feb 2019	Version 2.2 Release

Abstract

Seqrite Unified Threat Management Release Notes for version 2.2 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 2.2.1 version released on 20 Feb 2019

Product Name	Release Date	MD5 Checksum	Build Version
Seqrite Unified Threat Management	20 Feb 2019	4bf23ceaee6404db115e62c9596603b5	Build 2.2

New Features and Enhancements

IPS Enhancements

Granular configuration support for signatures on IPS- Enable /Disable based on Group defined.
Define priorities of the Signatures

Support for High Availability (HA)

The High Availability (HA) feature in UTM 2.2.x release ensures that the UTM appliance is available and has in-built redundancy (Active-Passive) The feature utilizes 2 identical UTM hardware appliances in which passive appliance will takes over in case active appliance fails.

The HA feature can be enabled on the T2 series hardware versions only.

Support for Centralized Management System (CMS)

Cloud base Management - Seqrite CMS is an integrated solution that allows the management and regulation of multiple UTM appliances deployed at different geographical locations. Administrators from any location can easily connect to Seqrite CMS to view the Appliance health.

- Dashboard - Single screens in which various critical pieces of information is placed in the form of widgets panels
- Remote Access Control (RAC) - To access and manage the console of an individual appliance directly from CMS
- Status - You can view the group hierarchy and underlying appliances. On selecting a group, the details for the registered appliance for that group

Support for ARP

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address (MAC) that is recognized in the local network. In the UTM appliance, the ARP cache table is displayed on the ARP page under the Network section. The following information is displayed on the ARP page:

- IP address of the connected device
- The corresponding MAC ID
- Interface on which that device is connected

- Type of entry whether complete, incomplete, dynamic or static.

You can view, search, add, and delete the entries displayed in the ARP table. You can also refresh the page or flush the contents of the ARP cache table. The table is updated dynamically or can be refreshed when required.

Support for Ability to download VPN packages directly from UTM

As part of this enhancement, Users can download the UTM VPN client package without any dependency on UTM Admin.

Enhancement in Consolidated Reports format

This is a specific enhancement to cater the reporting for UTM.
This feature provides:

- Support for Auto generated Monthly consolidated report for UTM in HTML format.
- Support for adding specific logo in Report.

Bug Fixes - UTM2.2

Sl #	Summary
01	Unable to view DHCP lease details under DHCP option on UI
02	Users’ are able accessible blocked websites as well.
03	PBR rule fails due to some error handling condition.
04	Unable to login into UTM using Super admin
05	Unable to fetch DHCP IP in LAN with Bridge Mode from router connected at Bridge WAN side
06	IPsec site to site VPN is not active when load balancing is configured at both sites UTM
07	HTTP Website shows 'Access has been Denied! ' while clicking on track the Shipment number in URL http://www.dhl.com/en.html

Known Issues:

The following table lists some of the important known issues to consider in version 2.2

Sl #	Summary of Known Issues
01	**High Availability:** Old Master UTM device remains master after some time. This is an intermittent issue.
02	**High Availability:** Failover in bridge mode might take 1 minute or more time
03	Time Quota policy applied on a group doesn't block https sites when MITM is OFF. By default, MITM is set to off in UTM. When Administrator configures time-based policy on a group, it does not work for https traffic by default. **Workaround:** Enable MITM for time quota policy to work on https sites.
04	**Admin console** ➢ Browser versions not supported IE versions such as IE8, IE9, IE10 and IE11 are not supported for Admin console. **Workaround**: Use recommended browsers as shown in Appendix section. ➢ Admin console access port Accessing UTM through port 543 does not display logs for BW Utilization, Live Web Usage & Live User Data Usage on Edge and Firefox browsers by default. **Workaround:** Use Google Chrome. For Mozilla Firefox, 1. Access the URL https://<ipaddress_of_utm>:9998. 2. Add exception when Security warning message is shown. 3. Now login to UTM console and access the page. This is one time setting and is not required to be done again for the same browser and UTM.
05	X-FORWARDED for HTTP header is not supported for HTTPS traffic in case of MITM OFF.
06	Unable to enter IPs subnet mask other than 24 in IP-wise group. If an IP range is with netmask 22, 16 etc. (anything non-24), the entire range cannot be added in the group. **Workaround**: Split the IP range into various sections of 254 IPs and add. For example, 10.10.1.1-10.10.1.254 and 10.10.2.1-10.10.2.254.

Important Points to Note:

Configuration of High Availability feature:

- Firmware upgrade, backup restore, and factory reset are independent from HA, these features work as is in previous versions. HA needs to be disabled first for Firmware upgrade, backup restore, and factory reset.
- HA should be enabled with different WAN IP address to avoid IP conflict after switching HA off.
- Access from the virtual IP will be lost if HA is turned off.
- Interfaces with any child interface should not be configured as dedicated interface.
- LA/Bridge interfaces should not be configured as dedicated interface.
- Default LAN-UTM SSH rule on UTM should not be altered for HA configuration to work.
- Secondary device will be in read only mode in PASSIVE state only. Configuration will be allowed if the device goes in FAULT state.
- HA configuration can only be edited by disabling it and reconfiguring it.

Configuration of CMS:

- Port: 9736 & Port: 8443 all traffic should be allowed [*for outside use, mentioned Ports should be allowed from LAN-To-WAN*].
- SHH Server should be whitelisted in the periphery firewall on WAN side.
- Please verify that the network in which UTM is kept is able to access https://www.apicmscloud.seqrite.com for CMS to work.

Captive Portal recommendations:

- For Captive portal logo –
  The recommended size for log jpeg image is 225 X 70 px

Following items are not in scope for High availability:

- Following sessions will break if Failover /Failback happens on the UTM system:
  - User transport session management
  - Admin session management
  - VPN User session management
- No Support for HA Clustering.
- Firewall state

- IPsec state
- IPv6 Support
- HA fail-over in case of DB corruption is not supported.
- Path monitoring for fail-over is not supported.
- Support for configuration sync-up for HA via CLI

Appendix

Recommended Browsers:

- Latest versions of Google Chrome
- Latest versions of Mozilla Firefox
- Microsoft Edge

Installation of UTM version 2.2.1

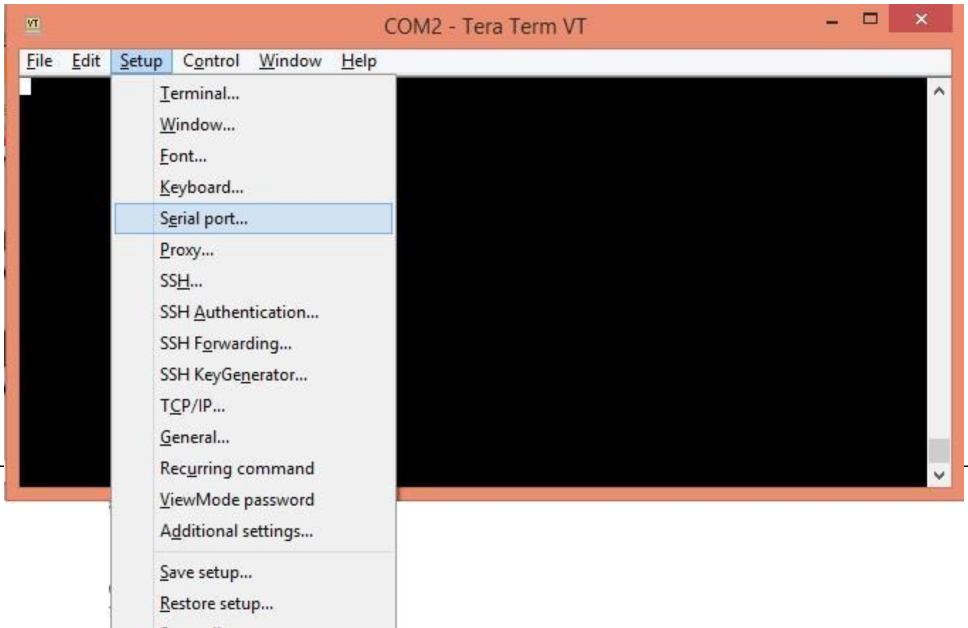
Using ISO

1. To install UTM 2.2.x, you need bootable USB drive. A 2.2.x bootable USB drive could be created writing the 2.2 ISO to the USB drive using tools such as Rufus.

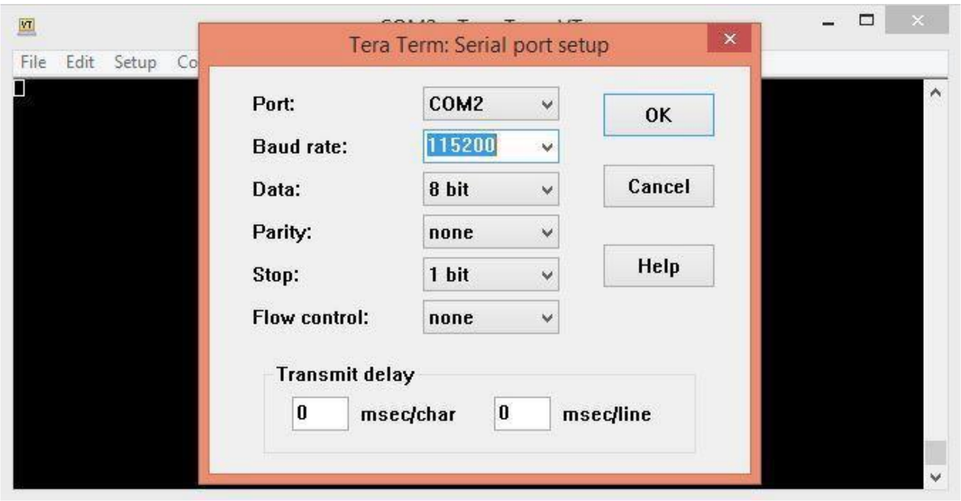
2. Once you have the 2.2.x bootable USB drive ready, plug it in USB port of UTM, attach console cable.

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

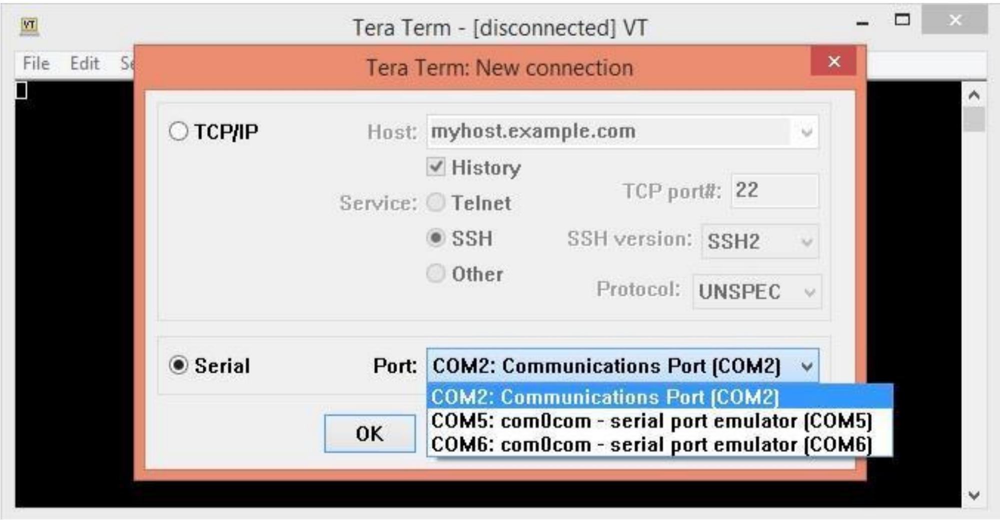


Tera Term: Serial port setup

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.



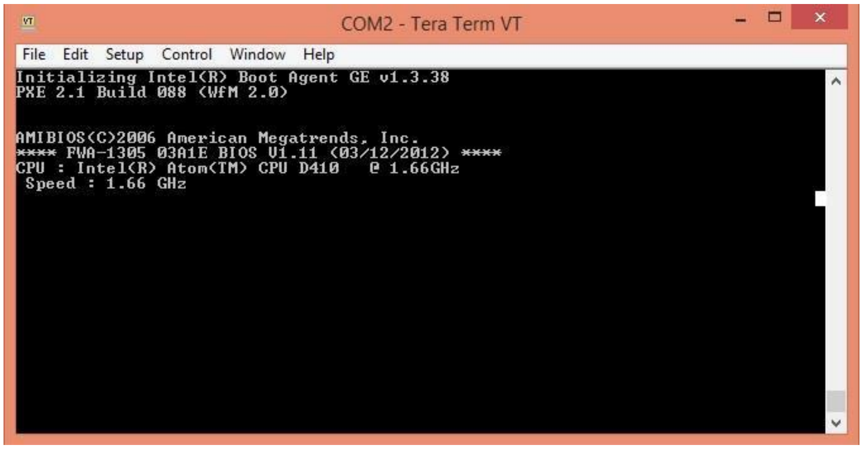
Tera Term - [disconnected] VT

Tera Term: New connection

○ TCP/IP
Host: myhost.example.com
☑ History
Service: ○ Telnet
● SSH
○ Other
TCP port#: 22
SSH version: SSH2
Protocol: UNSPEC

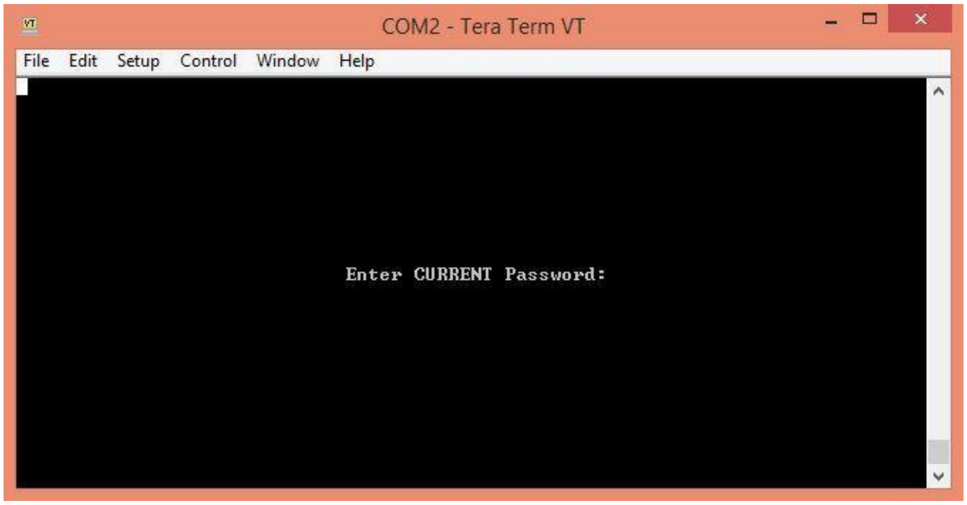
● Serial
Port: COM2: Communications Port (COM2)
COM2: Communications Port (COM2)
COM5: com0com - serial port emulator (COM5)
COM6: com0com - serial port emulator (COM6)

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



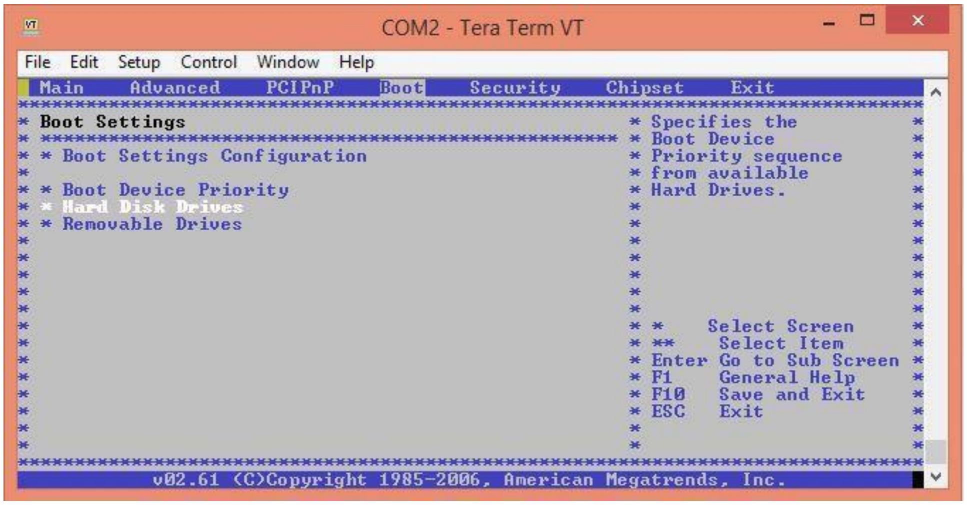
```
Initializing Intel(R) Boot Agent GE v1.3.38
PXE 2.1 Build 088 (WfM 2.0)


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.



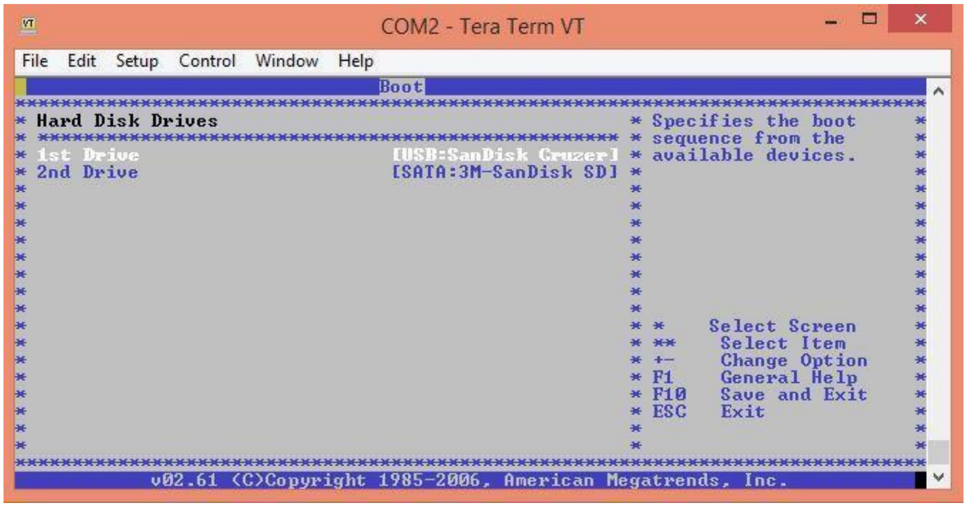
```
Enter CURRENT Password:
```

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



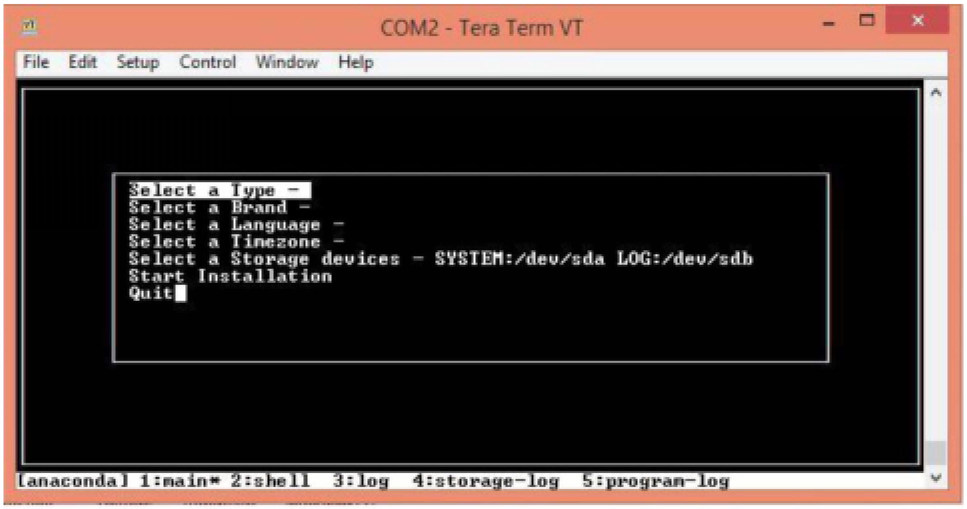
```
                                          Boot
********************************************************************************
* Hard Disk Drives                                         * Specifies the boot    *
* ******************************************************** * sequence from the     *
* 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.
```

IMPORTANT NOTE:

- If the above boot menus are not noted:
    - Please make sure that "UEFI" option is not selected for installation of UTM2.2.x
- **If there are further doubts, please check the embedded document below for more details**

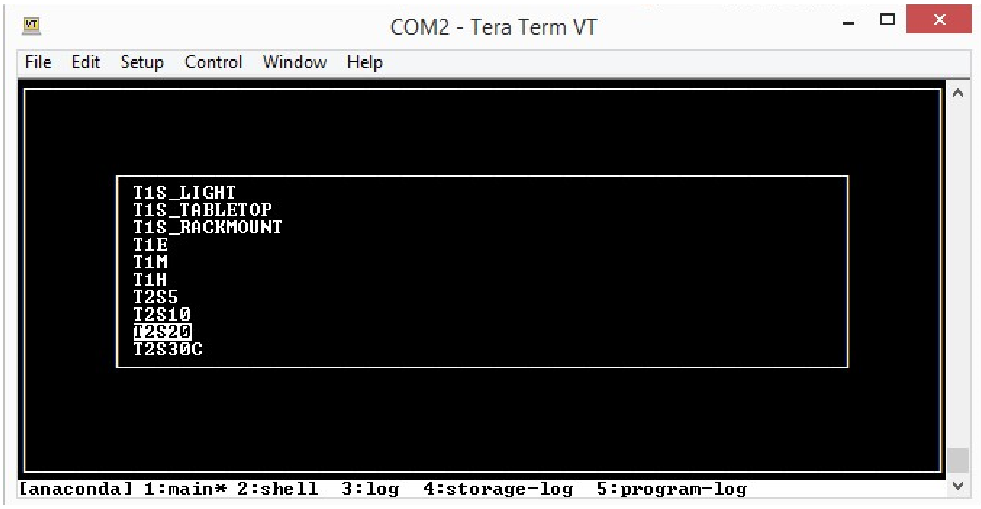
11. Save the changes and Exit.

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



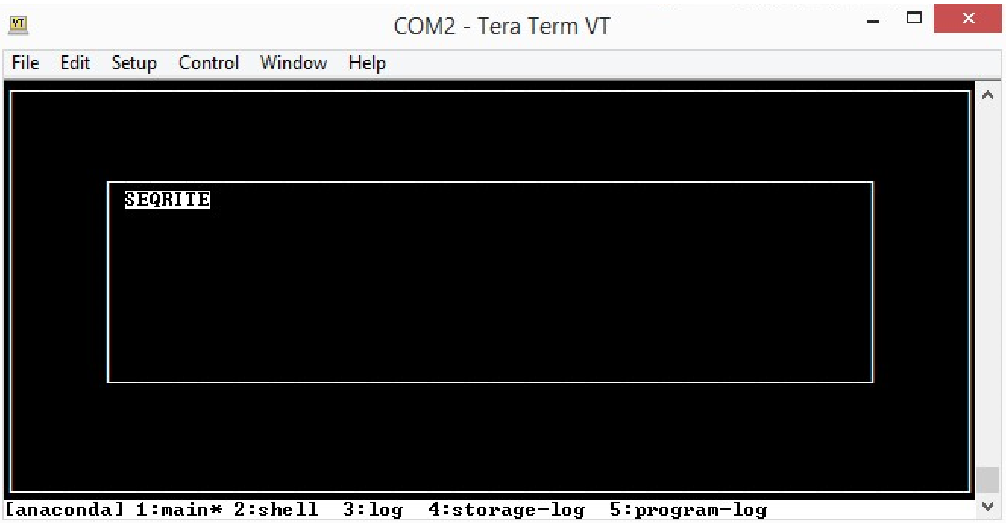
```
Select a Type -
Select a Brand -
Select a Language -
Select a Timezone -
Select a Storage devices - SYSTEM:/dev/sda LOG:/dev/sdb
Start Installation
Quit

[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.



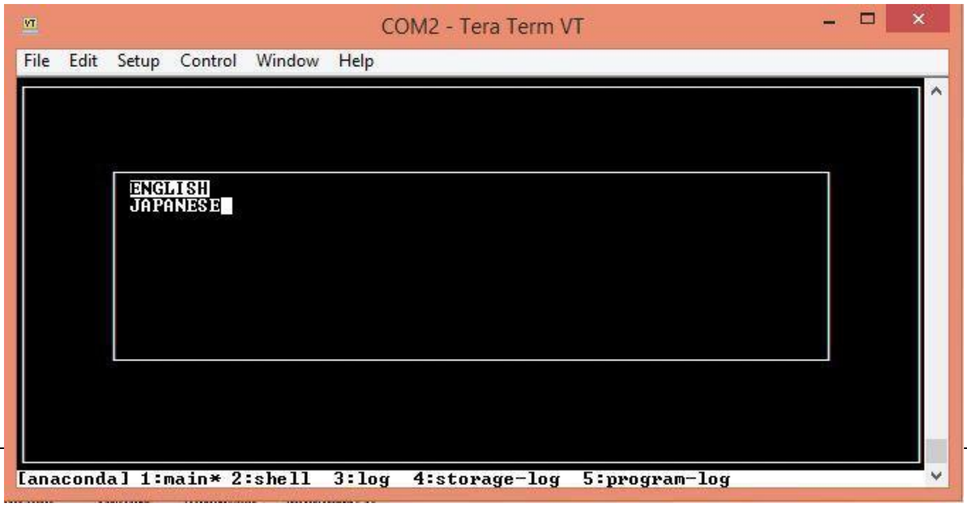
```
T1S_LIGHT
T1S_TABLETOP
T1S_RACKMOUNT
T1E
T1M
T1H
T2S5
T2S10
T2S20
T2S30C
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

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



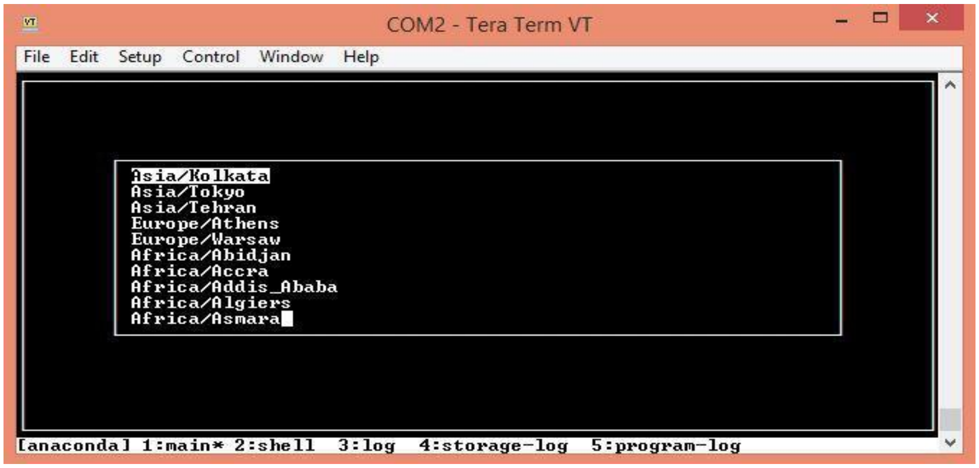
```
SEQRITE
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

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



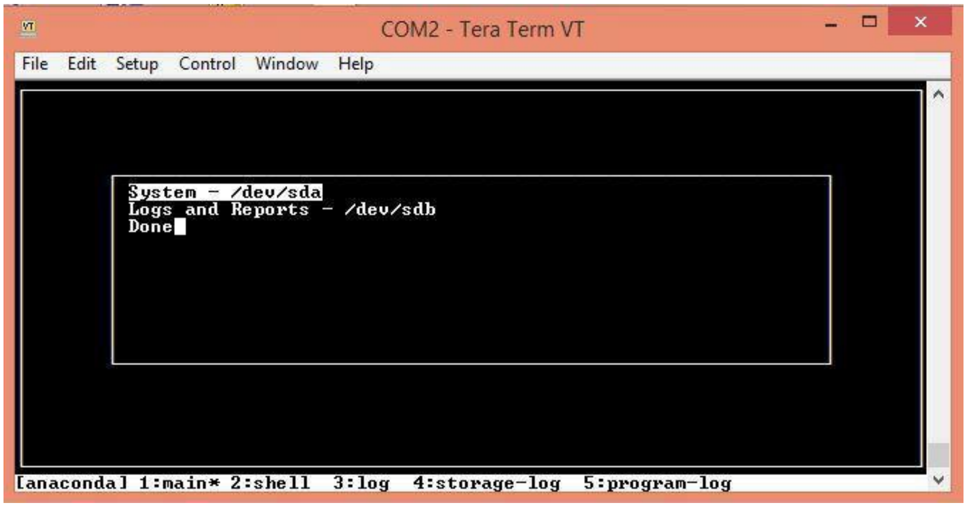
```
ENGLISH
JAPANESE
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

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



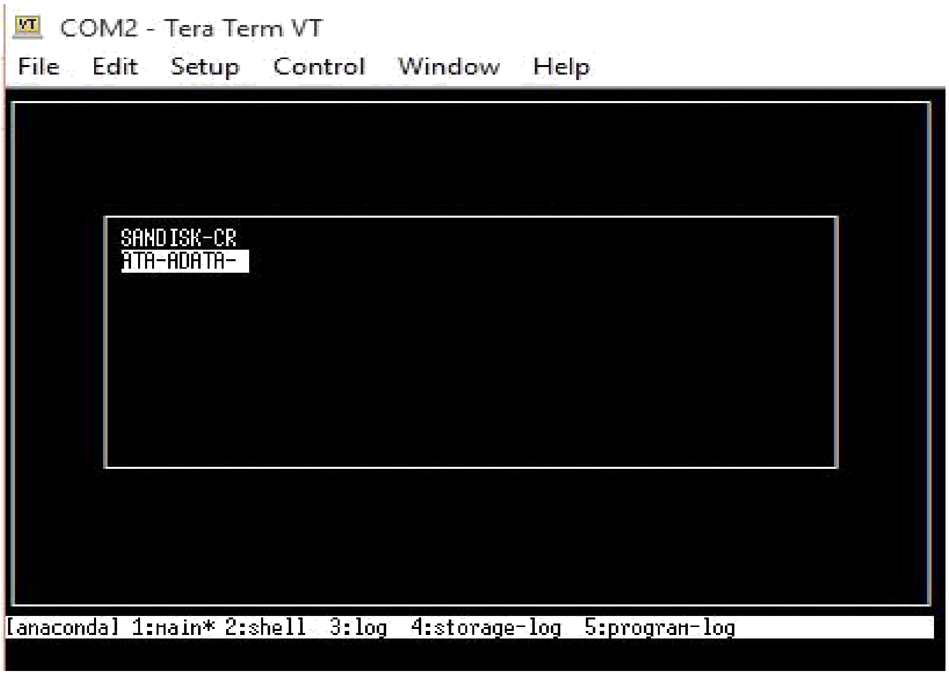
```
Asia/Kolkata
Asia/Tokyo
Asia/Tehran
Europe/Athens
Europe/Warsaw
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara

[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
```

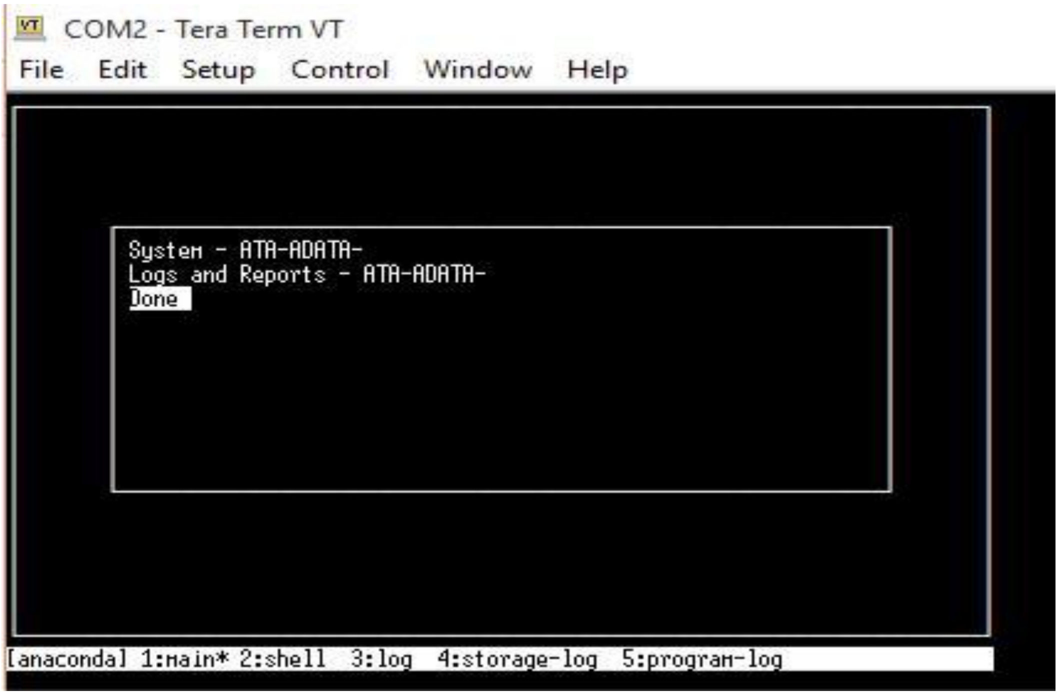
18. Select the same ATA device for *Logs and Reports* too. The screen would like the following for devices with Adata.



```
SANDISK-CR
ATA-ADATA-

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

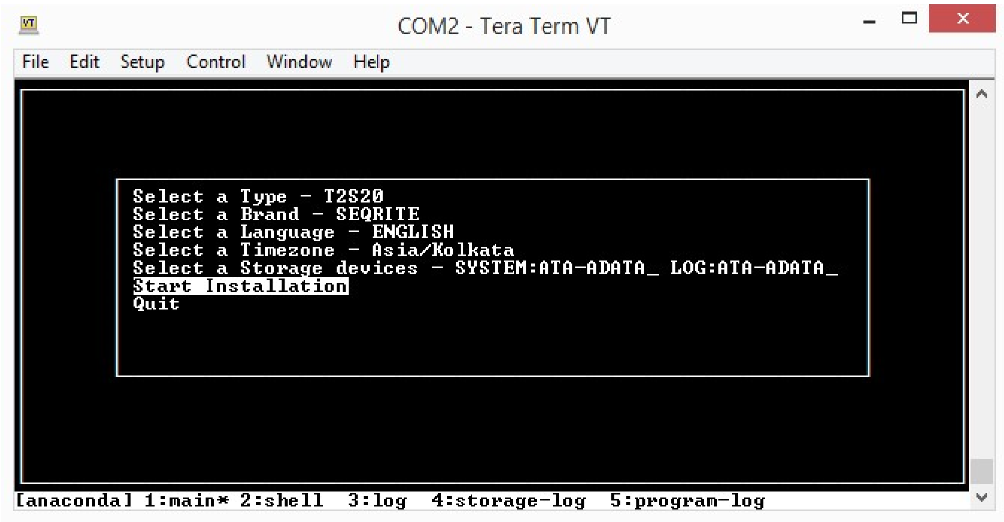
19. Note that devices with Cactus CF would have '*ATA-CACTUS*' while those with Sandisk (Old devices) would have 'ATA-Sandis' (not supported anymore) as the option. For T2M-250 with Intel SSDs, it would be ATA-Intel.

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

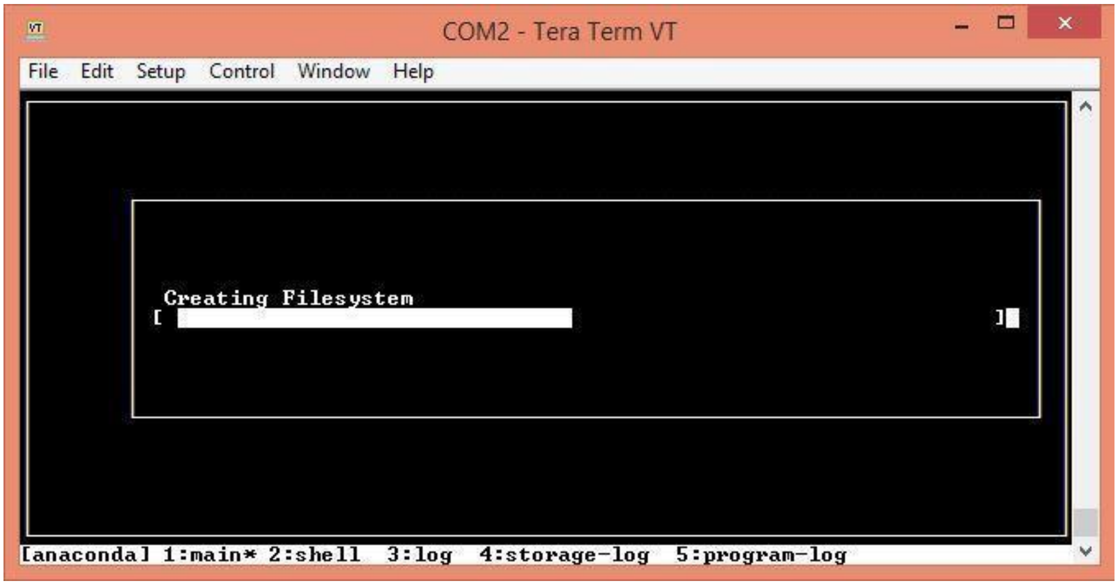


```
System - ATA-ADATA-
Logs and Reports - ATA-ADATA-
Done

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

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



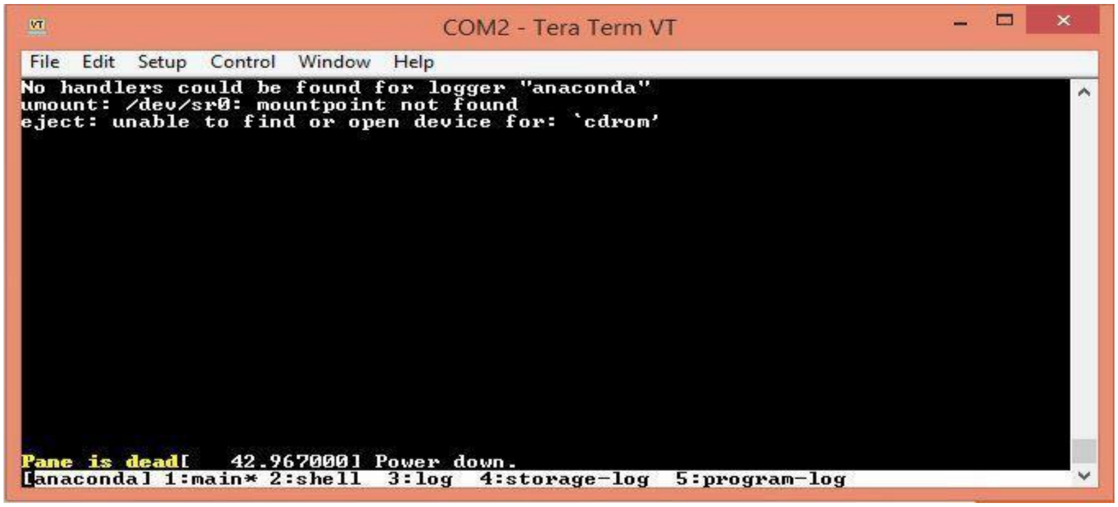
```
Select a Type - T2S20
Select a Brand - SEQRITE
Select a Language - ENGLISH
Select a Timezone - Asia/Kolkata
Select a Storage devices - SYSTEM:ATA-ADATA_ LOG:ATA-ADATA_
Start Installation
Quit

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



```
 Creating Filesystem
[                                                        ]

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

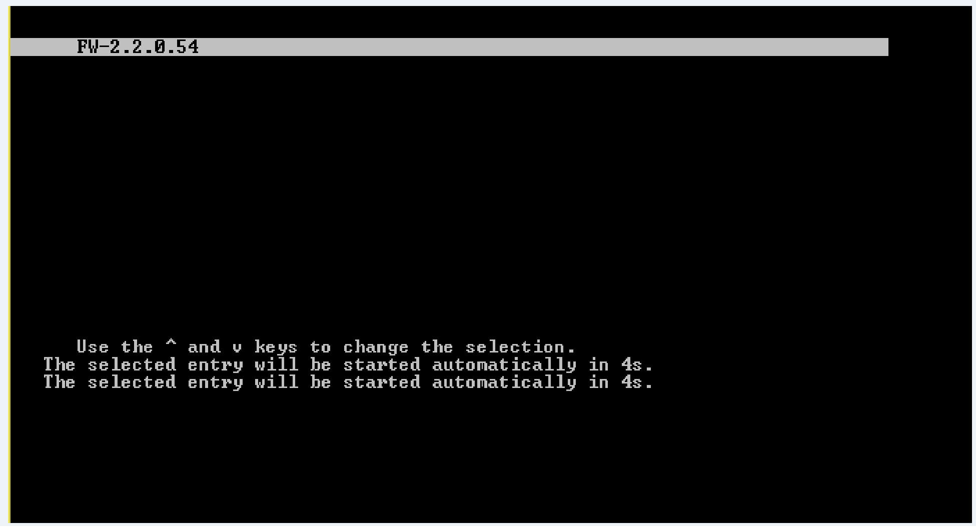
22. After installation is done, UTM will reboot and once again will go to UTM installation menu (As boot device priority remain same for USB). Once you see the menu, select on Quit. You would error for eject command saying ‘unable find or open device for: cdrom’. Ignore this message.

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"
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
```

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

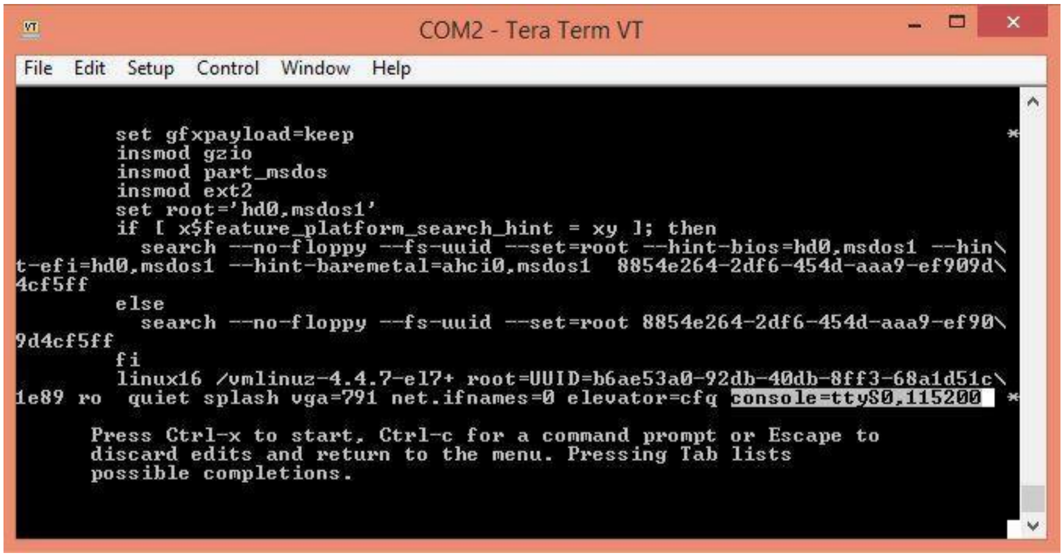


```
     FW-2.2.0.54






     Use the ^ and v keys to change the selection.
  The selected entry will be started automatically in 4s.
  The selected entry will be started automatically in 4s.
```

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 2.2

- T1S
- T1M
- T1E *
- T2S-5
- T2S-10
- T2S-30C
- T2S-30
- T2S-60
- T2M-100
- T2M-250
- T2E-500
- 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

All devices with 2.1.6.2 version installed can be upgraded to version 2.2.1.14

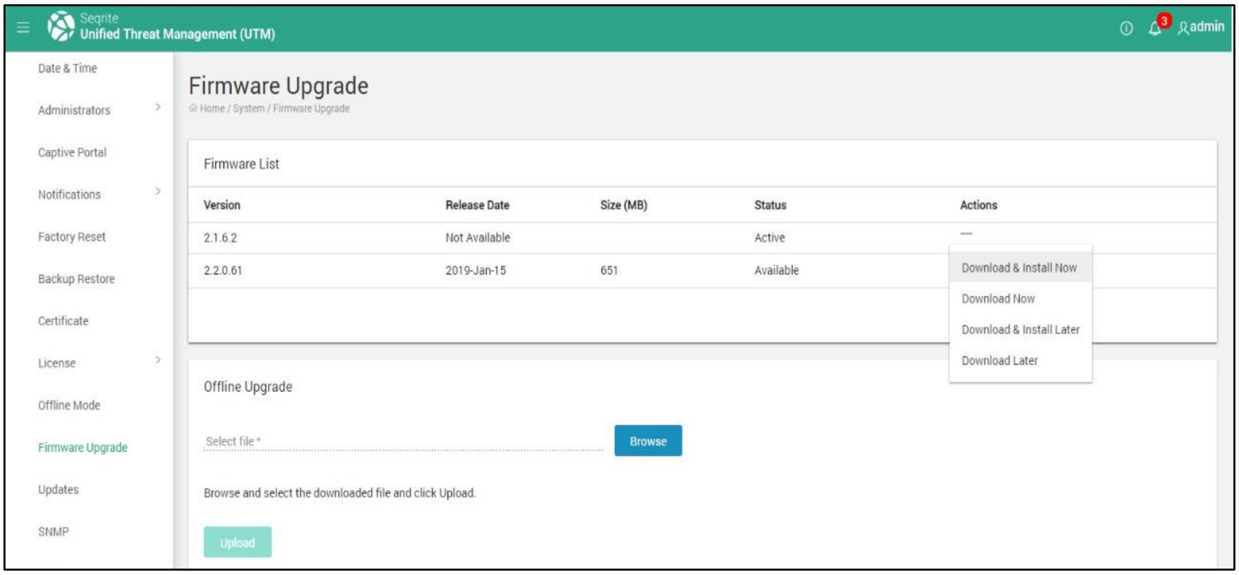
In order to upgrade to 2.2.1 version, administrator can follow two paths. The upgrade process would take around 25-30 minutes and would involve 2 reboots.

Note: -

- 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.

Online Upgrade

Login to the UTM as Administrator and go to the page System -> Firmware Upgrade. Under Firmware List, 2.2.1 version status would be shown as available. You could choose any of the actions to download and install the upgrade.



Firmware Upgrade

Home / System / Firmware Upgrade

Firmware List

Version	Release Date	Size (MB)	Status	Actions
2.1.6.2	Not Available		Active	—
2.2.0.61	2019-Jan-15	651	Available	

Offline Upgrade

Select file *

Browse and select the downloaded file and click Upload.

Offline Upgrade

You may want to choose Offline Upgrade, if the UTM device is in offline mode or is not connected internet. In this case, you need to download the upgrade package from Seqrite website and upload to the UTM.

For offline upgrade:

1. Visit the following URL
   https://www.seqrite.com/seqrite-offline-product-upgrades/

2. Select the Seqrite Unified Threat Management (UTM) product version.
3. Click on download button and download the file on your machine.
4. Login to Seqrite Unified Threat Management (UTM) using the admin credentials.
5. Go to the System → Firmware Upgrade page. In Offline Upgrade section, click on browse button.
6. Select the ".enc" file downloaded in step 3.
7. Click on Upload.

NOTE:

1. If the UTM devices are on 2.1 version lower than 2.1.6.2 then Admin must apply updates to bring it to 2.1.6.2 version so that upgrade to UTM 2.2 could be done.
2. If UTM device is on latest 2.0 version and to move to 2.2 latest version, the path should be as below:

   2.0 latest version → 2.1 latest version → 2.2 latest version

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/