Seqrite Unified Threat Management (UTM) 2.0

Release Notes

28th December 2017

Copyright Information

Trademarks

Seqrite is registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

License Terms

Installation and usage of Seqrite Endpoint Security 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

Build Information

Build 2.0.0.76 Version released on 05th Jan 2018

Product Name	Release Date	MD5 Checksum	Build Version	Build Virus Database
Seqrite Unified Threat Management	05 Jan 2018	260b035555f61ff2331dc5dc79fe5aa0	Build 2.0.0.76	28th Dec 2017

Please contact Seqrite Support Team for the 2.0 Build download link.

New Features and Enhancements

UTM 2.0 has been designed with a focus to bring in more stability and reliability apart from enhancing the design, security, UI and some of the existing features such as load balancing.

Here is a summary of what's new in UTM 2.0:

- New OS - Based on latest Linux kernel
- Redesigned easy to navigate and use Dashboard
- Re-organized left pane and menus are re-classified based on functionality
- Improved performance [UTM Throughput]
- Ability to configure and disable proxy for specific interfaces
- Configurable Link State Monitoring for Interfaces
- Enhanced IPSec VPN
- Added SSL VPN client support for Windows 8 and Windows 10
- PBR Failover
- Revamped Load balancing and Failover feature
- Concept of Policy introduced
- IPS signatures re-classified
- Better scanning options in IPS - Incoming/Outgoing, Request & Response
- More options to customize captive portal
- Default security policy (All devices blocked unless added into user-wise or IP-wise group)
- Online and Offline firmware upgrade
- Revamped and better Reports & Logs
- More diagnostic options
- Bug Fixes

New OS - Based on latest Kernel Version

- UTM 2.0 version is based on newer kernel version **4.4.7**. As it is based on newer Kernel version, various software modules/libraries in the system are all comparatively newer versions which means better performance and security as they come with many fixes for the performance and security bugs compare to the older versions of those softwares.
- The new firmware also comes with the **ext4 filesystem**. This reduces the IO on the storage thus increasing the life of CF (Compact Flash) and SSD along with providing the reliability of a journalling filesystem.

New Dashboard

- The Dashboard has changed and does not display Top Viruses or Top Intrusions or Top policy breaches found, instead it displays the count of viruses, intrusions and policy breaches for the day. Clicking on each of the display card displays the detailed report for each of those categories.
- The CPU usage shows instantaneous CPU usage instead of average over a period of time.
- System status card now also shows CPU load average and current time and uptime.
- Device Information card introduced which would give the user details on the device such as Software Version, Hardware Model, Product Key etc. In version 1.8, this information was not easily available.

Reordered Left Pane and menus are better classified

- Internet Settings is now Proxy settings in Network menu. Network → Proxy.
- IPS, AV, Mail Protection and ACC available under Security.
- Authentication Server (for AD integration) available under User Management.

Improved Performance [UTM Throughput]

- UTM 2.0 comes with improved performance. The performance tests conducted in the labs show a 30% improvement in UTM throughput when compared with previous version.

Configure and disable proxy for specific interfaces

An option is now available to configure port for proxy for each interface. Proxy can also be disabled for each interface.

Configurable Link State Monitoring for Interfaces

Link state monitoring module is used to check the status of a link. Link State Monitoring is now configurable where an admin can choose whether to monitor the status using ICMP or using DNS and also can configure which server to be used for ICMP or DNS.

IPSec VPN feature enhanced

- NAT traversal for IPSec VPN traffic supported
- IKEv2 Support which was not there in 1.8.X version
- Support introduced for additional encryption algorithms apart from the ones supported in earlier versions. The following are the new additions:

  Encryption Algorithm:- Serpent, Camellia

  Authentication Algorithm:- SHA2 256, SHA2 384, SHA2 512

  DH Group:- 15(DH3072), 16(DH4096), 17(DH6144), 18(DH8192), 22(1024 bit, sub 160 bit), 23(2048 bit, sub 224 bit),24(2048 bit, sub 256 bit)

SSL VPN client support extended to Windows 8 and Windows 10

- UTM VPN client is now also supported on Microsoft Windows 8 and Windows 10 OS apart from Windows 7. However, Windows XP is no longer supported.

PBR Failover

- There is an option to add primary and secondary target for PBR. If routing through primary fails, traffic can be routed through secondary target.

Load balance and Failover revamped

- True failover is now implemented. You can have 2 interfaces working in Active-Passive mode. Only when the first interface goes down the second would come up.
- Failover check logic is configurable. Click on Advanced and edit the settings if you want to tweak on how sensitive the failover need to be.

Concept of Policy introduced

- UTM 2.0 has new concept of policy introduced. For example, if you want to create a group named HR - whom you want to give access to social networking and another group named RnD to which you do not want to, this is how you will go about doing it.
  a. Create two groups - one named HR and another named RnD.
  b. Add user or IP ranges to define it as userwise or ipwise.
  c. Go to Policy → URL Categorization.
  d. Under Policies, click on plus sign to create a new policy.
  e. Configure the categories you want to be allowed and blocked.
  f. You can notice there that you can apply time category across URL categories. i.e you may allow a category between specific timings (like FB allowed during lunch time) etc. To do this you need to create a Time Policy first under Policy Menu.

IPS Signatures re-classified

- IPS signatures are reclassified. Please go through the list and see the description. If you have any queries you can write to utmsupport@seqrite .com
- Better scanning options in IPS - Incoming/Outgoing, Request & Response
- Earlier there were only 3 main options in IPS. Scan traffic from WAN, from LAN to WAN and to scan inter-LAN traffic. However, in UTM 2.0 more options are provided. For example, earlier there was no option to scan traffic from WAN side that comes in as part of response. Now it is made available. Both incoming and outgoing traffic have options to scan Request as well as Response. These options could affect performance and hence unless sure, stick to the default. More options chosen, more security but lower performance.

More options to customize captive portal

You would see the menu for this option under System → Captive Portal. The options are self-explanatory. You may change the logo, colors etc. of the captive portal page apart from some of the options of the page from this menu

Default security policy (All devices blocked unless added into username wise or IPwise group)

- This is one important change you need to be aware of. In UTM 2.0, a device need to be in either username-wise or IP wise to access anything routed by UTM. i.e. for

accessing internet or inter-LAN devices, a PC device need to be part of UTM group (username-wise or IP-wise). This was not the case in 1.8 or earlier (except for http(s) traffic).

- If you find unable to access anything although you have a seemingly correct configuration, first check - Is your device configured in a group? If no - are you logged in ? If answer for both is 'no', then do add the device to IP-wise group or login to UTM as user-wise.

Online and Offline firmware upgrade

One of the major features being provided in UTM 2.0 version is the facility to upgrade to next version of UTM software without reinstallation. This upgrade of firmware could be done over the air (Online upgrade) or offline upgrade- where the upgrade package could be downloaded onto your laptop and then uploaded to the device to upgrade.

Revamped Reports & Logs

Improvement in performance, new charts etc. are done in this area. The Logs and Reports would be loading faster in UTM 2.0 when compared with previous versions.

More diagnostic options

- To provide better support, we have added couple of small features into UTM 2.0.
  a. You may check the category of the website under Support → Diagnostics
  b. You may 'Bypass security Policy" to convert device to a plain router with no security policies applied to quickly confirm if UTM is blocking any traffic. Once this Bypass mode is switched on, UTM will not block any traffic from LAN-WAN. If traffic is still being blocked or inaccessible, you may check other factors.
  c. You may choose destination interface while testing Ping and traceroute.

Known Issues

The following table lists some of the important known issues in version 2.0 along with workarounds for those issues.

Sr. No.	Summary
1	**When installing UTM 2.0 from a USB, an error is shown during installation.** **Workaround:** The error that says "eject: Unable to find or open device for :'cdrom'. This is not a bug but a warning from OS. This error message could be ignored and the installation still succeeds.
2	**URL CATEGORIZATION**: **A policy such as 'allow Facebook during specific times' [Time based] policy does not work.** **Workaround:** The time category works only for block action for '*category based*' policy. To allow the domain during specific times, create a policy to Block the whole category – *'Social Networking'* and whitelist the domain *'facebook.com'* with the required time category attached to it.
3	**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
4	**URL CATEGORIZATION**: **Block page is not shown for HTTPS websites in case MITM is off.** No access denied page is received when https page is denied and MITM is off. The browser would keep spinning till timeout.
5	**Firewall live connections page does not respond under heavy load**
6	**Unable to edit existing IPS custom rule until SID is changed.** When admin tries to edit an existing IPS custom rule pattern, it throws error. **Workaround:** Change the corresponding SID within the custom rule while changing the pattern to edit the rule

7	**Internet quota gets auto reset when the UTM time is changed manually.**
8	**Host header forgery detected errors seen in UTM logs while accessing HTTPS websites when MITM HTTPS Scanning is enabled.** **Workaround:** This happens in case of using MITM HTPPS Scanning. Could be resolved by switching off MITM and moving to the default mode. An attacker (or malware installed on innocent end-user computer) puts a fake IP for popular website like www.google.com or www.facebook.com in hosts file on PC behind the proxy. Once an infected PC requests the webpage in question, a cacheable fake response poisons the cache. In order to prevent such scenarios (as well as some others) Seqrite UTM has implemented a mechanism known as **Host Header Forgery Detection**. In short, while requesting an URL from origin server IP as hinted by the client, UTM makes independent DNS query in parallel in order to determine if client supplied IP belongs to requested domain name. In case of discrepancy between DNS and client IP, the transaction shall be flagged as non-cacheable to avoid possible cache poisoning, while still serving the origin response to the client. However, this also leads to false positives in case of websites with multiple IP addresses. **We recommend configuring the same DNS servers in UTM which are configured in local systems or you can use UTM LAN IP Address as first server in your local systems.**
9	**IPv6 is not supported on bridge interface**
10	**Internet quota works only for HTTP(S) traffic**
11	**Admin UI is not supported on Mobile.**
12	**Domains hosted on multiple IP addresses when added to Direct Domain list is not accessible sometimes.** This is because during the process of adding to direct domain list whichever IP was resolved to the domain first is added to the direct domain list.
13	**Seqrite UTM 2.0 installation requires complete reinstallation of the OS on UTM Appliance. We do not support any existing configuration migration from 1.8.X OS to 2.0.** It is recommended that Admin takes necessary configuration documentation backup to reconfigure UTM 2.0 again with same set of policies. Admin can export user's configuration from 1.8.x OS version in CSV format and restore the same in 2.0 OS to get same set of users and passwords configurations in Seqrite 2.0.OS.

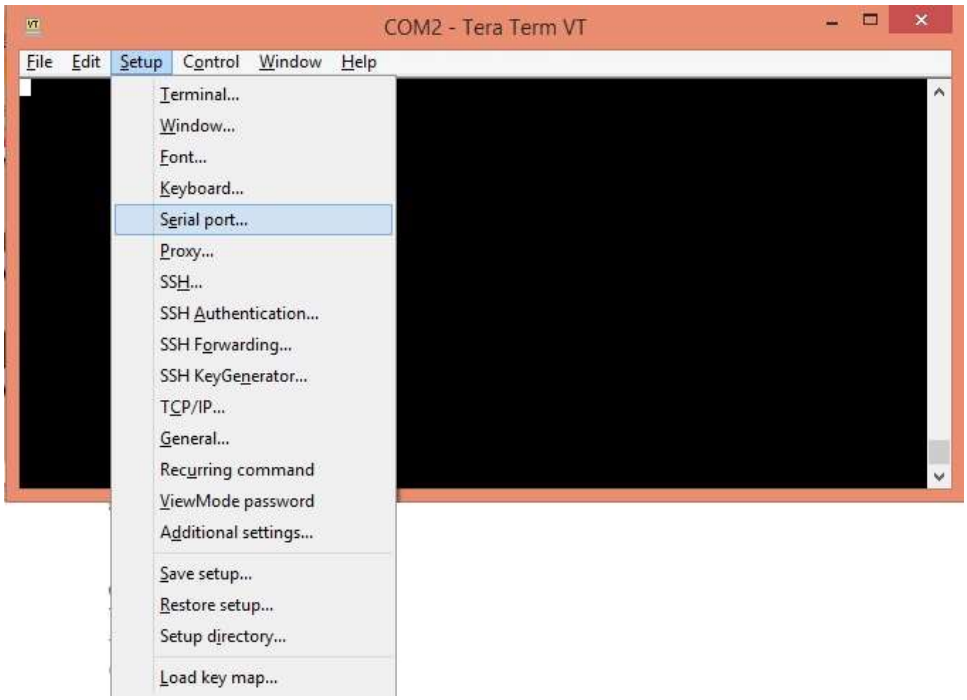
Bug Fixes

Some of the Post Release defects found in UTM 1.8 have been addressed in UTM 2.0:

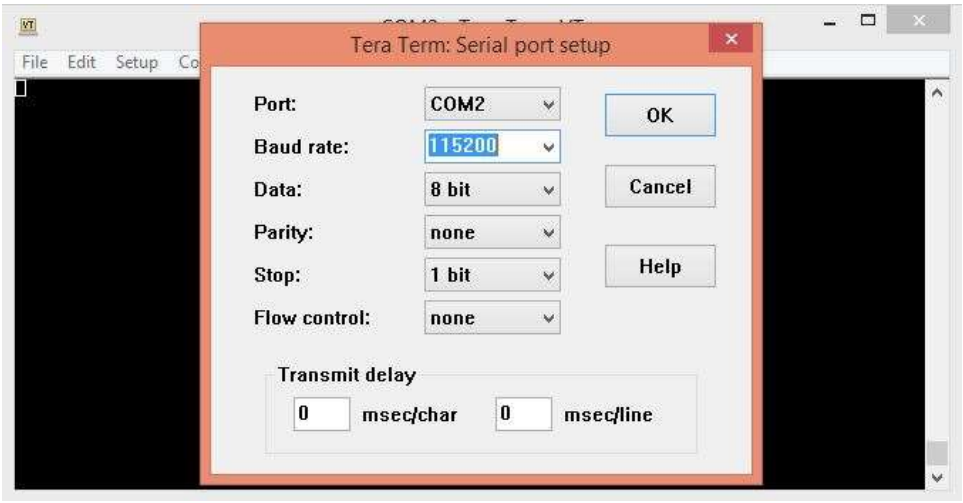
- Bug ID: 51116: When clicked on logout option in UTM user-login page then browser shows message that "page is loading please wait" and browser is not responding.
- Bug ID: 50850: Unable to access UTM from other WAN IP if default route ISP is down.
- Bug ID: 50694: Unable to connect Remote SSL VPN client on IPhone 6 and 5s.
- Bug ID: 48196: Unable to receive email due to mail protection ON when Server needs NTLM authentication support.
- Bug ID: 48594: PBR is not working as expected with version 1.8.4.23
- Bug ID: 45138: Unable to save Administration>SMTP setting due to "-" character in user name
- Bug ID: 44632: After license expired, Http & Https websites are not accessible in groups.
- Bug ID: 40291: WAN IP is not getting renewed in DHCP with ACT India ISP due to DHCP Timeout
- Bug ID: 39680: Firewall report cannot be exported in PDF format
- BugID: 39805: Unable to access specific links under website "http://helpdesk.worldfashionexchange.com/bugs.aspx"
- Bug ID: 36404: DIA IP are not getting priority if same IP in a group
- Bug ID: 27457: In load balancing traffic is going from secondary line having NA weightage

Appendix – Installation steps

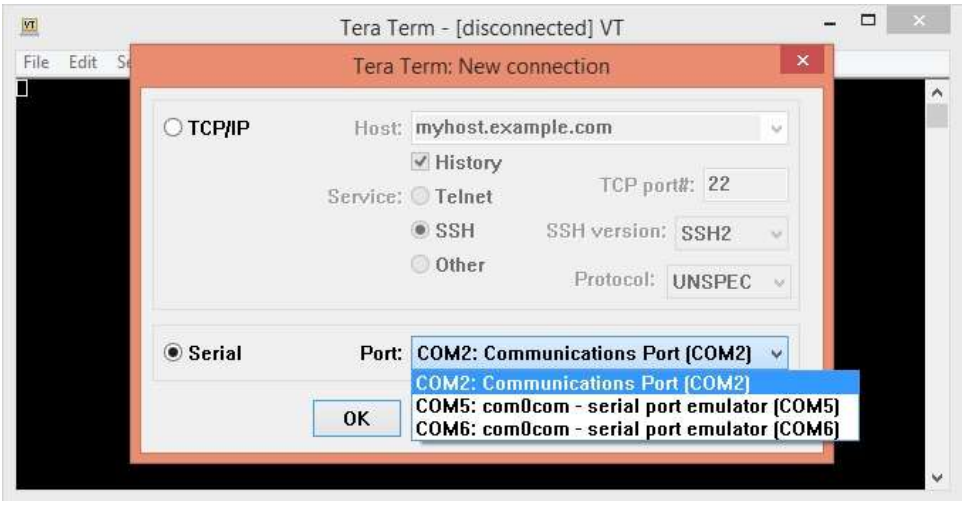
1. Contact Seqrite Support Team for the latest 2.0 OS build download link.
2. To install Seqrite UTM 2.0, you need bootable USB drive. A 2.0 bootable USB drive could be created writing the 2.0 ISO to the USB drive using tools such as Rufus.
3. After you have the 2.0 bootable USB drive ready, plug it in USB port of UTM, attach console cable.
4. Use Tera Term or Putty on MS Windows and Minicom for Linux to connect to the UTM device.
5. Open Tera term and select Serial port (ex: COM2: Communication port).



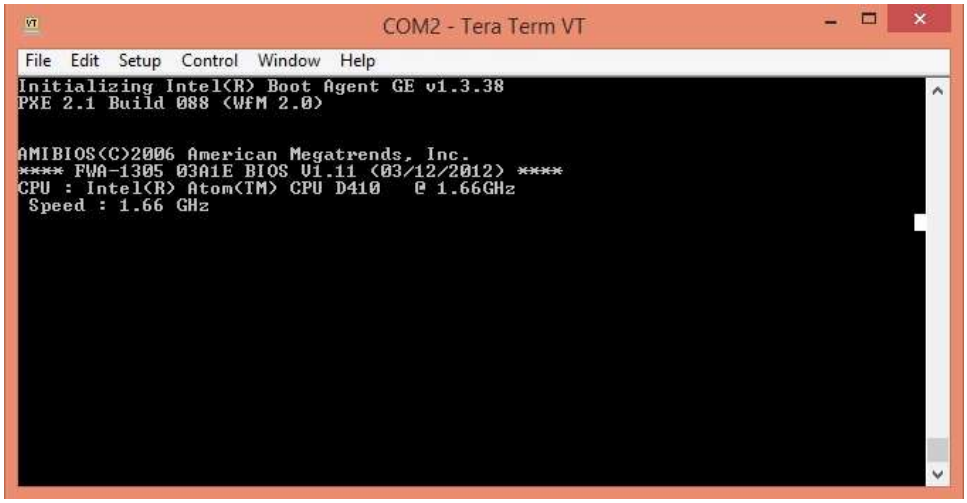
6. Configure baud rate by selecting Setup -> serial port



7. Select baud rate here as 115200.

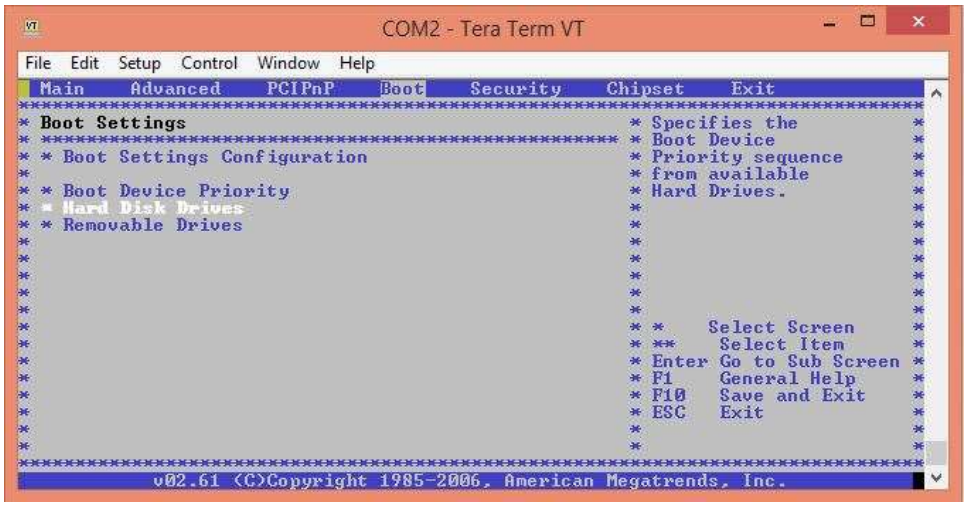


8. Now power on the UTM. You would see the screen as shown below:

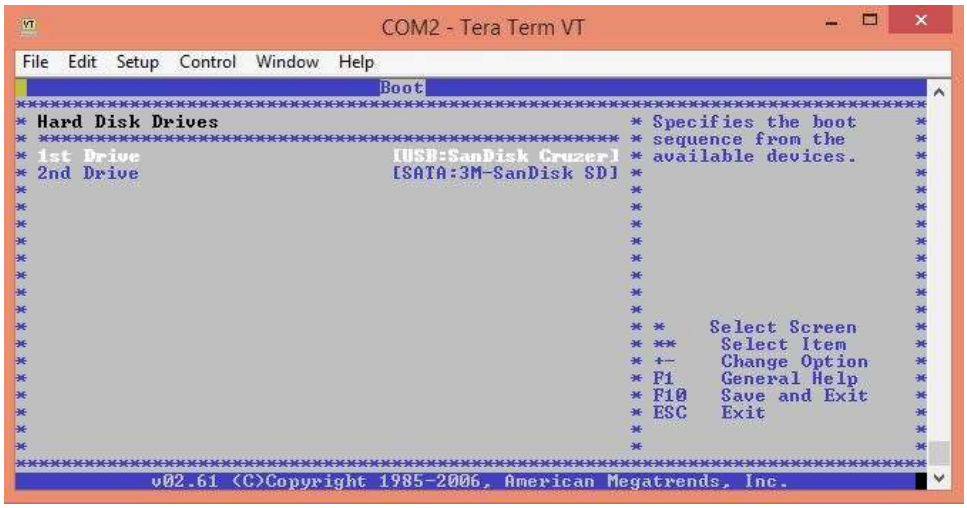


9. To select USB drive as first boot priority, hit 'Delete' button to enter into Seqrite UTM BIOS. Enter the BIOS password as “#3a1Q”.

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

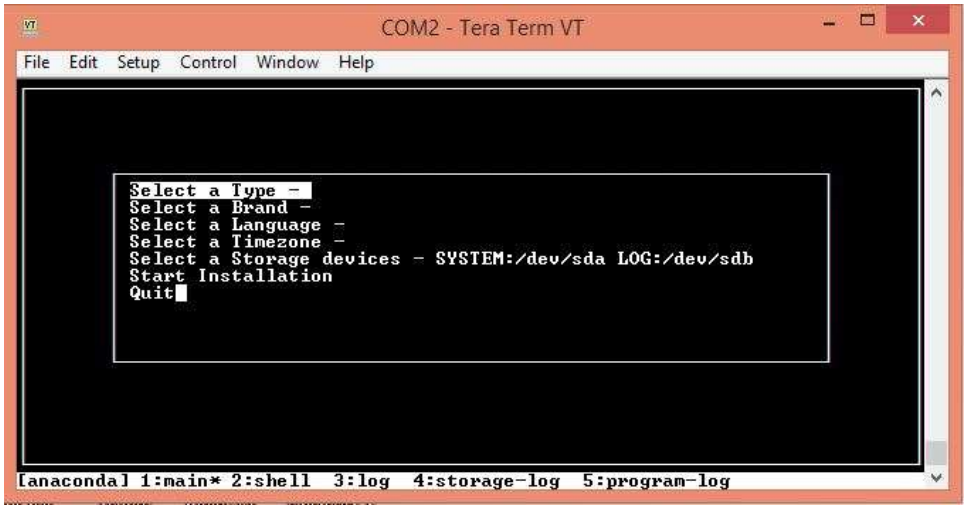


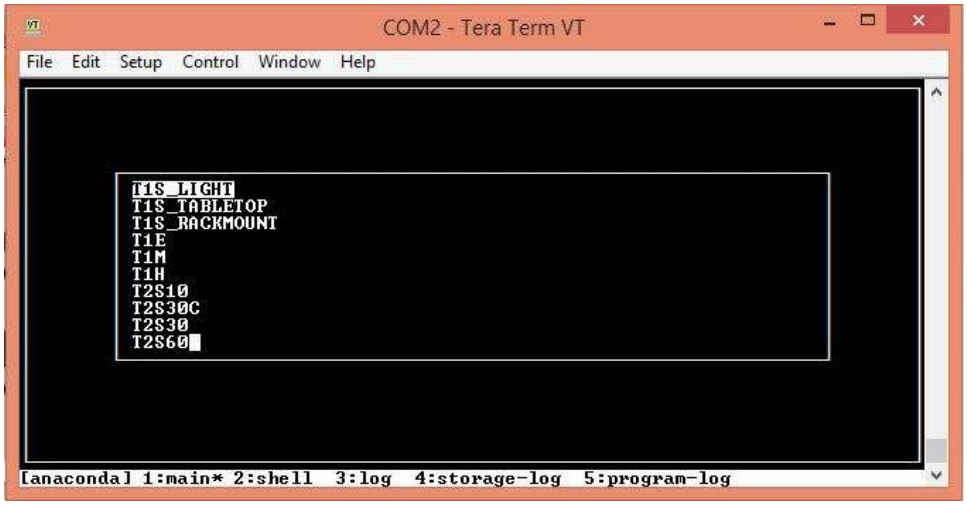
11. Choose the USB drive as the bootable drive



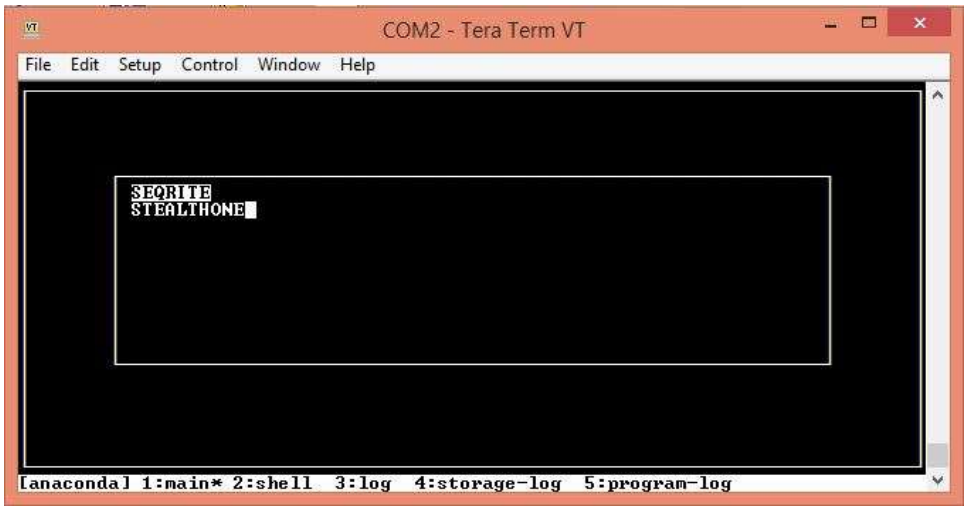
12. Save the changes and Exit.
13. Now reboot the device and you should see installation menu. Options seen are: Hardware Type, Brand, Language, Time zone and Storage device.

14. Select the hardware type. For example, for T2S-30 device choose, T2S30 option. Please contact technical support if you are not sure about your Model number to select from available options.

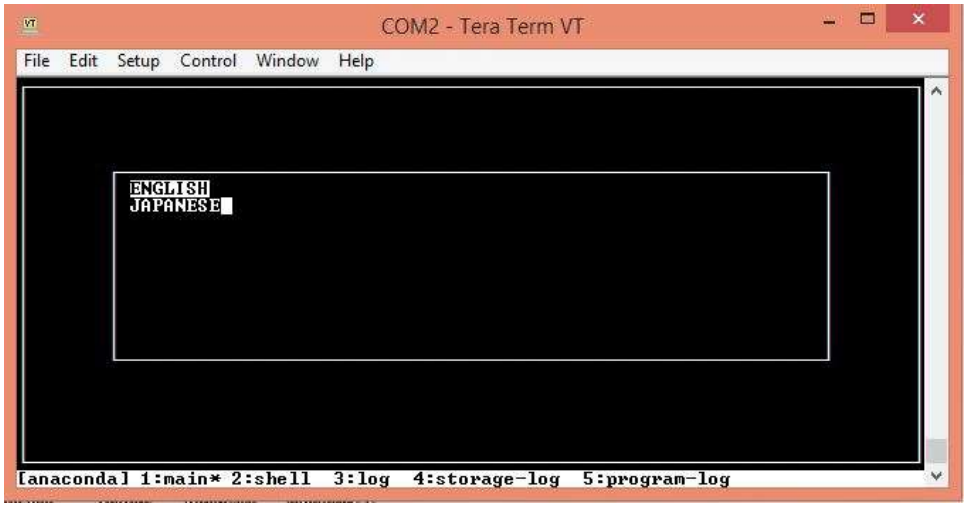




15. Now go to ‘Select a Brand’ and choose “SEQRITE” to install Seqrite UTM.

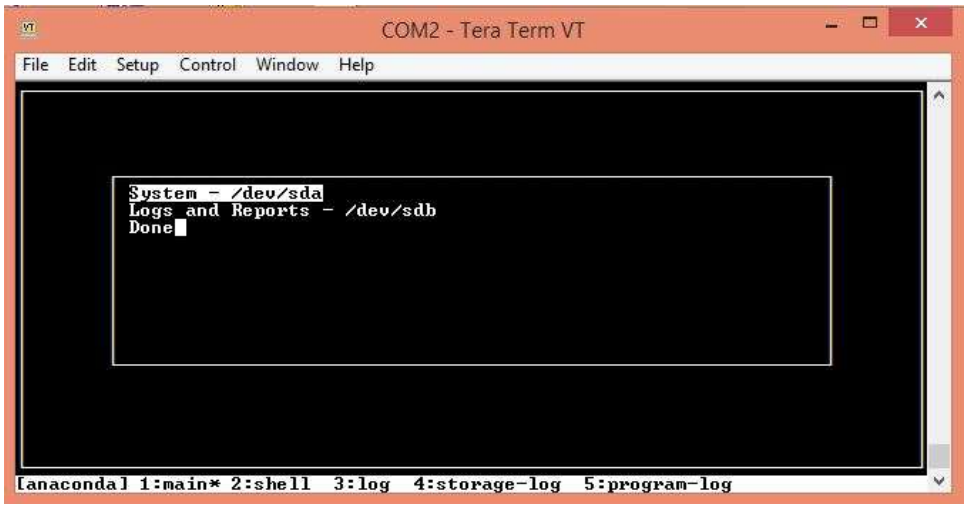


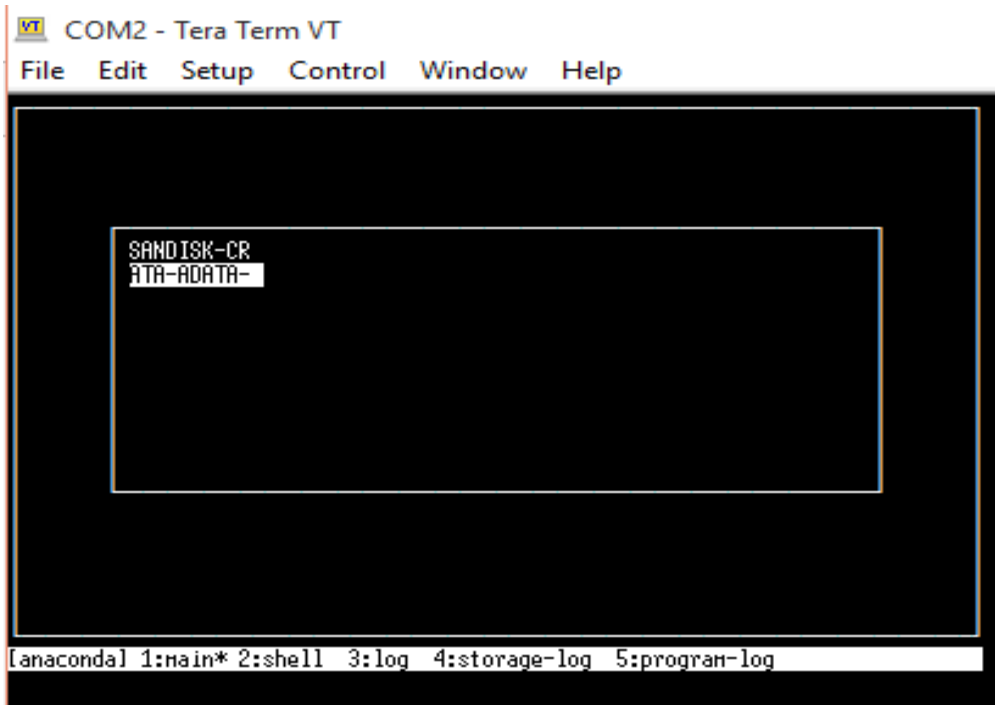
16. Now choose ‘Select a Language’ and select *English*.



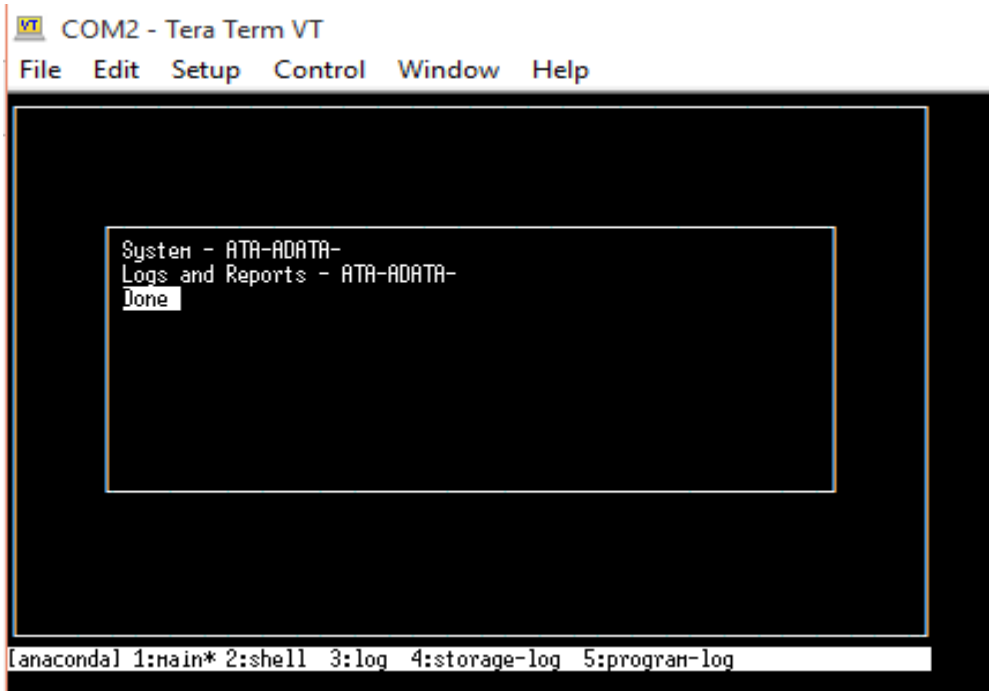
17. Go to *Select a Time zone* and select *Asia/Kolkata* for Indian time zone.

18. Choose 'Select a storage device' and select option that has prefix "ATA-" for System storage.





19. Select the same ATA device for *Logs and Reports* too. The screen would look like the following for devices with Adata storage in appliance.



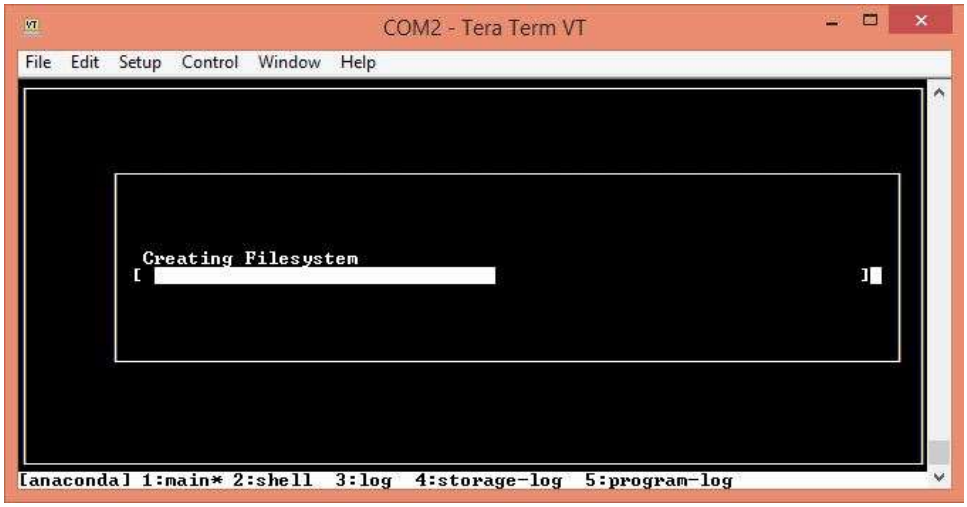
20. Note that devices with Cactus CF would have '*ATA-CACTUS*', while those with Sandisk (Old devices) would have 'ATA-Sandis' (No longer supported) as the option. For T2M-250 with Intel SSDs, it would be ATA-Intel.

T1X Series appliances with Sandisk CF (First Generation Devices) would have ‘ATA-Sandis’ as the option.

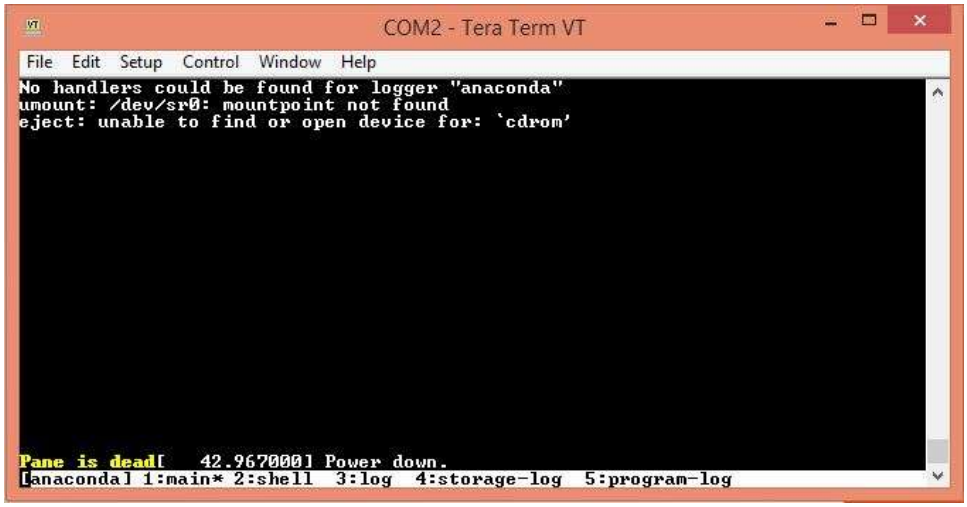
Note: CF or SSD of at least 16 GB is required to install Seqrite UTM 2.0 OS.

21. Click on **Done** to exit from storage device menu.

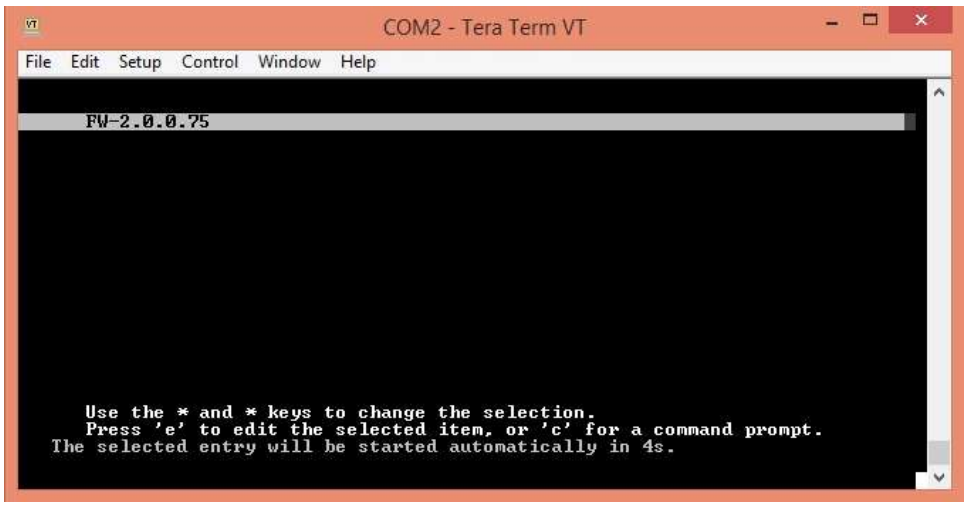
22. Verify all the values selected. Now select Start Installation.



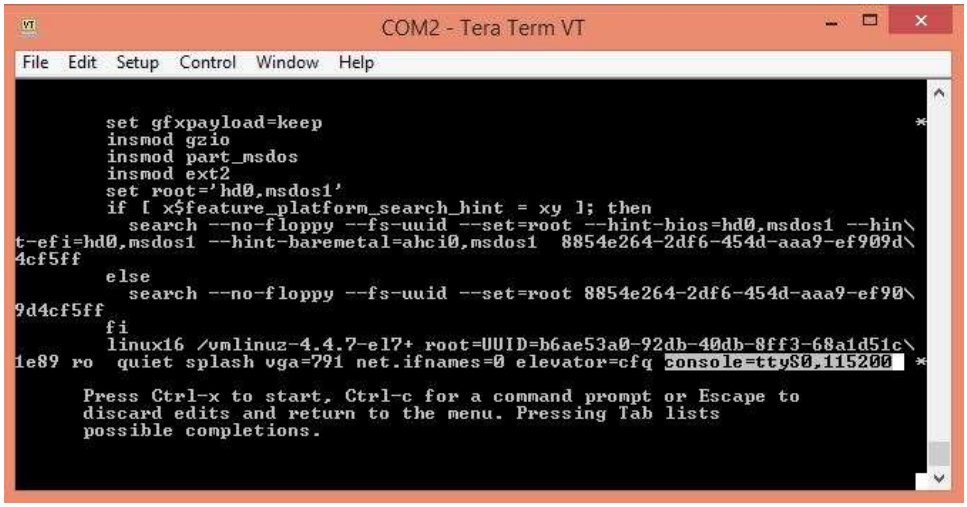
23. After installation is done, UTM will reboot and once again will go to UTM installation menu (As boot device priority remain same for USB). Once you see the menu, select Quit. You would error for eject command saying ‘unable find or open device for : cdrom’. Ignore this message.



24. 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:



25. Wait till UTM reboots two times and then login prompt will appear. That concludes the installation.
26. 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.



27. 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.

28. Once login screen is visible, login as *admin* to change IP address from the default if required.
29. 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 UTM release 2.0

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