SEQRITE

Empowering Businesses with **Right** IT Security

Seqrite Unified Threat Management 2.1

Release Notes

July 2, 2018

Copyright Information

Trademarks

License Terms

Contents

Revision History

Version	Date	Comment
1.0	2 July 2018	Version 2.1

Abstract

Seqrite Unified Threat Management Release Notes for version 2.1 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 2.1 version released on 02nd July 2018

Product Name	Release Date	MD5 Checksum	Build Version
Seqrite Unified Threat Management	2nd July 2018	faeddeb5d18faea442e5a9b410d11fcc	Build 2.1

New Features and Enhancements

Support for Syslog

Seqrite UTM now supports logging to a remote syslog server. All logs from UTM would be directed to the configured syslog server and no log would be present in the UTM after the configuration is enabled. Seqrite UTM can support up to 2 syslog servers simultaneously. Syslog is supported over TCP, UDP and TLS.

Support for SNMP

UTM now supports SNMP protocol. You can now monitor Seqrite UTM using an SNMP manager. SNMP protocol versions V1, V2c and V3 are supported. SNMP is supported on Bridge, VLAN, Alias and Bond (Link Aggregation) interfaces too.

Live Utilization Logs and Reports

The following 3 new live features in Logs and Reports are now available for better administration and troubleshooting.

- ### Live Web Usage Logs

  This feature lets you (admin) monitor the URLs being accessed by live users. You can also search for patterns (such as IP, URL etc.) to narrow down the displayed information.

- ### Live Data Usage of Top 10 Users

  You can view the list of users who top in data usage. Any user downloading or uploading huge amount of data and is in the top 10, would show up in this list. As an admin, you can regulate the bandwidth usage using this feature.

- ### Live Bandwidth Utilization

  As an admin, you can gain insight into the link utilization for each of the interfaces. In case any link utilization is seen more than the available bandwidth, you can take the necessary action.

Historical Bandwidth Utilization

As an admin, you can view the historical link utilization over a period of 30 days.

VPN Failover

If WAN link failover is configured, then VPN IPsec site-to-site connection could be configured to fail over on the same WAN links.

Dynamic IP support in site-to-site IPSec VPN

In this feature, site-to-site IPSec VPN connections using link having dynamic IP would not require reconfiguration at remote end whenever the link IP address changes.

The IDs would be used as the main identifier for connection using provided options besides IP address. The IDs could be of type:

- IP Address
- Distinct Name
- Email ID
- FQDN Name

MTU and MSS Support

UTM now allows an administrator to change the MTU and MSS values for an interface. This feature is supported only via CLI.

CLI interface statistics view for admins

As an admin, you can view the various interface statistics such as Rx, TX details, packets dropped, errors etc. with the option provided under Troubleshooting -> View Interface statistics in CLI.

Automatic Logout of Users [Global logout and Forced User Logout]

As an admin, you can enforce logout of users based on:

- Duration i.e. logout users after X hours
- Time i.e. logout users at a specific time such as say 12:00 in the midnight
- Logout all users on reboot of the device

The first 2 options are available at group level as well as global level.

DoS & DDoS Attack Prevention

As an admin, you can now prevent DoS/DDoS attacks by using the feature provided under Firewall. Following 3 protections are available:

- SYN/TCP Flood
- ICMP Flood
- UDP Flood

User Level Bandwidth Control (Individual Mode)

Earlier UTM version supported Shared Mode policy for bandwidth control. i.e. if 10 Mbps is set as bandwidth for users within a group, then 10 Mbps divided by number of users is the bandwidth that each user would get. With 'Individual Mode', an administrator can ensure each user would get 10 Mbps provided there is enough bandwidth.

Consolidated Report over Email

If email notification is configured, you can get a consolidated report of the day by midnight, summarizing device details such as Memory, CPU usage, Disk usage, Policy breach attempts count etc.

Bug Fixes

Here is the list of bugs that have been addressed in UTM 2.1:

Sr No	Summary
1	IPS module is not detecting nmap scan from WAN to UTM.
2	Deleting a firewall rule deletes another firewall rule with similar rule name.
3	URL categorization service is set to disabled by default.
4	Antivirus-Mail protection service status showing down on dashboard even after enabling this service.
5	Browser page keeps spinning for denied HTTPs websites in case MITM is off.
6	License page shows version as 2.0.0.76 although 2.0.1.3 is applied
7	IP-MAC binding is ignored when the IP is present within DHCP scope also
8	Unable to mac bind IP address if its already present in leases list
9	Bandwidth usage reports does not match with actual usage

Known Issues

The following table lists some of the important known issues in version 2.1 along with workarounds for those issues.

Sr. No.	Summary
1	**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.
2	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.
3	Not all 4G USB dongles and hotspot devices from vendors such as Vodafone, Idea, Reliance and Airtel are currently supported. **Workaround**: Admin could use Airtel 4G dongle (Model: Huawei E3372), which is tested and supported so far.
4	A policy such as 'allow Facebook during specific times' need to be specified as an exception for a generic category block policy. The time category works only for block action for '*category based*' policy. For example, 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.

5	Internet quota gets auto reset when the UTM time is changed manually. If Internet quota is already set for users in a device and had been under use, changing the time of the device manually would reset the quota. It is advised to set the date-time to correct value during the initial setup of the device.
6	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.
7	X-FORWARDED for HTTP header is not supported for HTTPS traffic in case of MITM OFF.
8	**IPS Custom Rules** To edit existing IPS custom rule, edit the SID and use another unique SID.
9	Enable dead peer detection to make IPsec VPN Failover work on IKEv2.
10	IPv6 is not supported on bridge interface.

Appendix

Recommended Browsers

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

Installation of UTM version 2.1

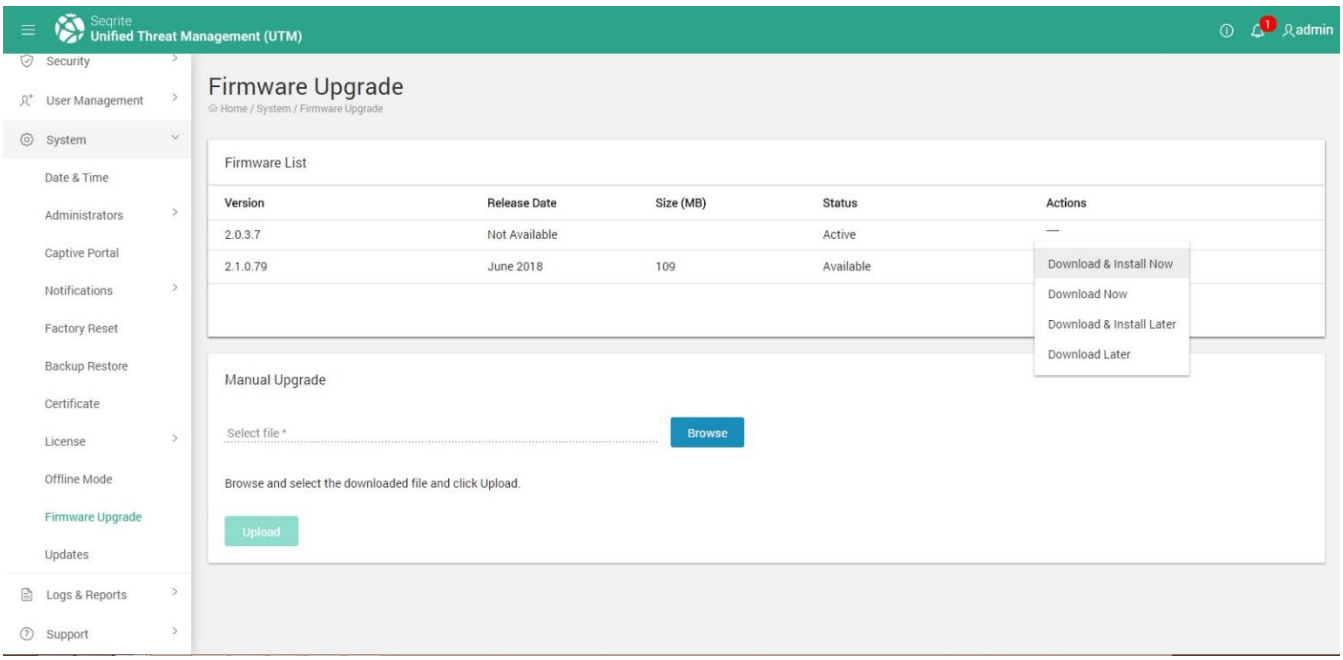
Via Firmware Upgrade

All devices with 2.0.3 version installed could be upgraded to version 2.1. In order to upgrade to 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 and 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, 2.1 version status would be shown as available. You could choose any of the Actions to download and install the upgrade.



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.

If the devices are on version lower than 2.0.3, then administrator must apply software updates to bring the UTM device to 2.0.3 version so that firmware upgrade could be done.

Supported Devices

Following hardware devices are supported in 2.1

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

*Supported only on devices with storage size 16 GB or higher.

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/

For more information on the deployment you can refer the Seqrite UTM User guide at

https://www.seqrite.com/resources/cat/manuals/