SEQRITE

Seqrite
UNIFIED THREAT MANAGEMENT (UTM)

Administrator's Guide

Version 2.4.0

Copyright & License Information

Trademarks

License Terms

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

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

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Chapter

1

About Seqrite Unified Threat Management (UTM)

In today's world of increased security threats, administrators depend on multiple security solutions such as firewall, intrusion preventions systems, anti-virus etc. Seqrite Unified Threat Management (UTM) also known as Seqrite UTM is an integrated network security product that provides network administrators with all the security solutions in one device thus reducing the complexity.

Seqrite UTM helps administrators with single point of administration, monitoring and logging. Seqrite UTM saves on the time and cost required to deploy and monitor multiple security solutions.

Seqrite UTM Features

Seqrite UTM is a UTM solution that combines various security solutions into a single security appliance. Seqrite UTM provides the following protection features:

Protection Feature	Description of area of operation
Antivirus	Prevents, detects, and removes malware, including but not limited to computer viruses, computer worm, Trojan horses, spyware and adware. It attempts to repair an infected file or delete any virus infected file.
Anti-Spam	Automatically scans all the content and eliminates spam and phishing mails, thereby protecting your system against any phishing and spam attack.
Firewall	Permits or denies network traffic based upon certain rules used to protect networks from unauthorized access while permitting legitimate communications to pass.
Web/URL Filter	Filters web sites as a pre-emptive security measure to protect the network and prevent viewing inappropriate web sites or content.
Intrusion Prevention System	Detects and prevents intrusion to protect your network. Protects your

About Seqrite Unified Threat Management (UTM)

Protection Feature	Description of area of operation
(IPS)	system from hackers who can sneak into the system.

Additionally, Seqrite UTM provides the following features that facilitate a secure working environment:

Features	Description
Dynamic Routing using OSPF and BGP	Dynamic routes can be learned using OSPF and BGP. A dynamic routing table is created, maintained, and updated by a routing protocol running on the UTM.
User based policy management	Lets you apply seven different policies at user level. Provides you a tighter control as compared to group level policies.
Centralized Management System (CMS)	With UTM release 2.2 onwards, now you can view and configure your registered UTM appliances from a Centralized Management System console remotely. You are also notified of the latest infections, breaches and other related information of the UTM appliances on the CMS. Note: CMS license has to be purchased separately to avail CMS services.
High Availability	High Availability (HA) feature in UTM 2.2 release ensures that the UTM appliance is available at all times and has in-built redundancy and reliable crossover. Note: You have to purchase another UTM appliance of the same configuration as your existing appliance to avail HA service. HA can be configured only on T2 or appliances of higher configuration.
Mail Protection	Scan secure SMTP and POP3 email traffic.
Virtual Private Network (VPN)	Provides remote offices or roaming users with secure communication access to their organization's network over a publicly accessible network (Internet).
Bandwidth Management	Optimizes bandwidth usage by allowing allocation of bandwidth. The allocation can be done on the basis of usage among groups, thus saving bandwidth cost of the company.
Dynamic Host Configuration Protocol (DHCP)	Seqrite UTM acts as a DHCP server to allocate IP addresses to host saving configuration time of the IT administrator.
Load Balancing	Allows multiple ISPs to be used by Seqrite UTM. This feature allows traffic to be balanced across multiple ISP lines based on weightage and priority.

About Seqrite Unified Threat Management (UTM)

Features	Description
IP Port Forwarding	Allows remote computers to connect to a specific computer or service within a LAN.
Content Filtering	Allows you to filter web sites and allows you to create a whitelist of URL and domains that your network can access. You can similarly create a Black list of Web sites, URLS, and domains and stop access to them.
Logs and Reports	Provides comprehensive logging and reporting with a user-friendly web-based configuration.
Automatic Link Failover	Automatically diverts the data traffic from inactive ISP to active ISP lines in case any of the ISP lines fail to perform.
Policy Based Routing	Provides facility to make routing decisions based on administrator specified criteria. If network traffic passing through is satisfying the provided criteria, traffic will be forwarded through a target network interface link or target gateway.
Application Classification and Control	Using this feature, you can control access to applications by configuring rules as required to allow or block access to applications.

Chapter

2

Registration Wizard

Seqrite UTM appliance requires license registration and network configuration prior to operation. On successful login through web interface of Seqrite UTM, the Registration wizard is displayed. This wizard helps you to configure network interfaces, DNS, set appliance date and time, set appliance password, and complete the registration process.

Use the Option buttons on the upper right side of the wizard:

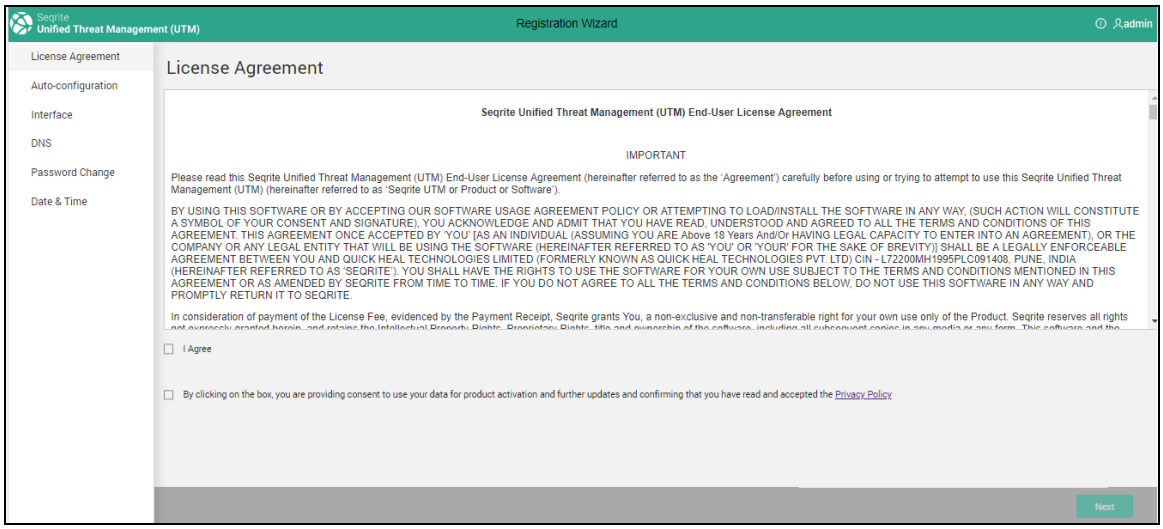
- Help: View help files which guides you to use the Seqrite UTM.
- System Information: To generate the system information that may be requested by support team. (A password protected PDF file sysinfo.qht is generated).
- Diagnostics: Helps you collect debugging information of the different modules in Seqrite UTM.
- Shut Down: Lets you power down the appliance.
- Restart: Allows you to restart the appliance.
- Logout: Helps you to log out of the appliance.

The steps listed below will help you in setting up the network configuration and registering Seqrite UTM.

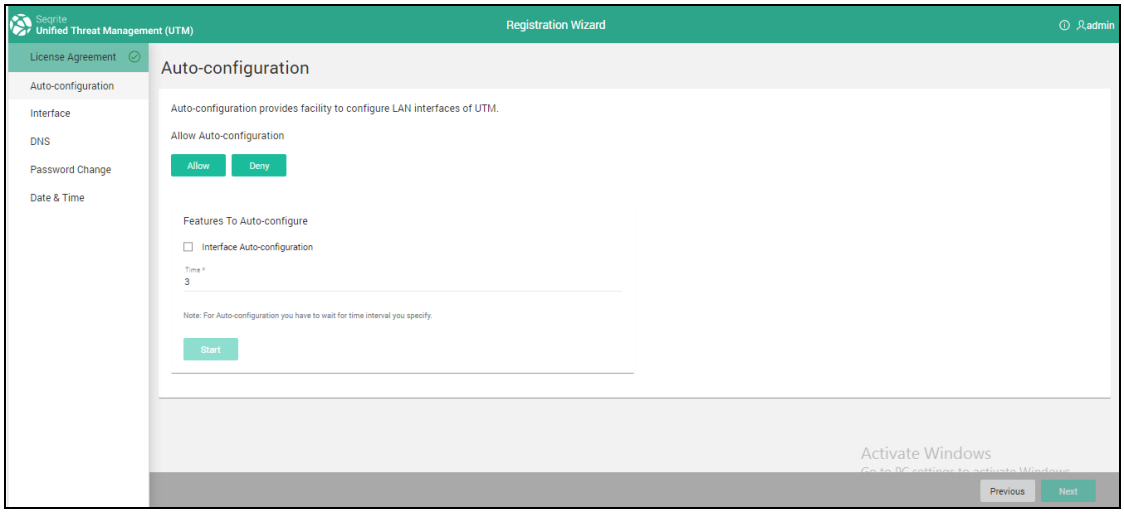
License Agreement

The License Agreement screen is the first screen that appear when you logon to Seqrite UTM for the first time.

Registration Wizard



1. Read the License Agreement carefully and select the **I Agree** check box to accept the terms and conditions.
2. Click the next checkbox to agree to provide your consent for data use and then click **Next**. The Auto Configuration screen is displayed.



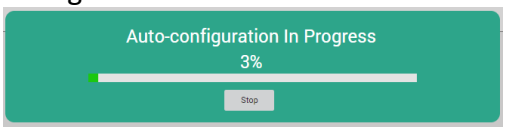
Configuring the Interfaces

After you agree to the license terms and click Next, the Auto Configuration screen appears. You have the following two options:

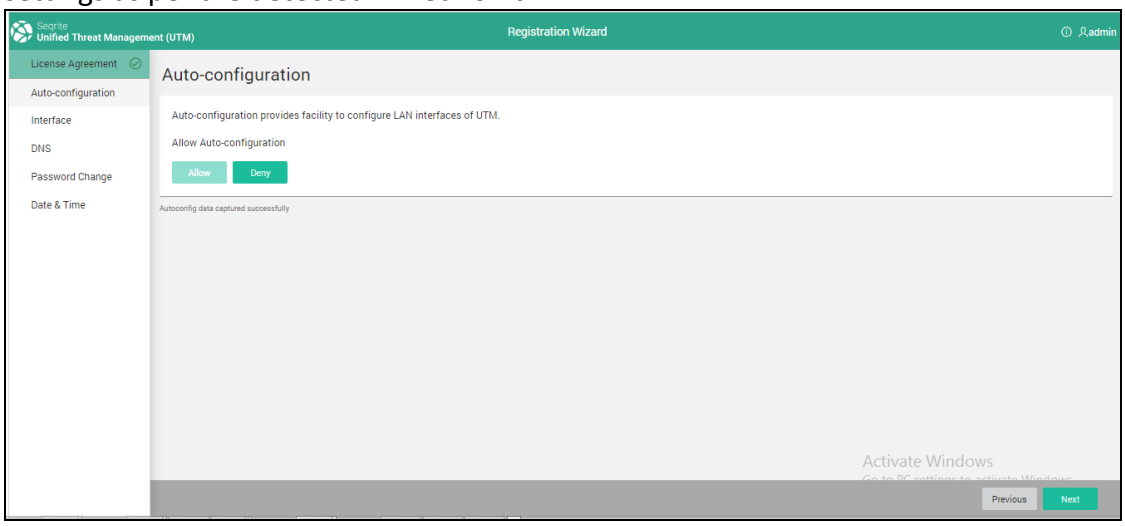
- Allow (Auto configuration): To automatically detect which IP network addresses are in use and configures the interfaces automatically for these networks.
- Deny: To manually configure the interfaces that are detected. You can also edit a listed interface or add a new one.
  Note: The Interfaces with internet connectivity are indicated in green color.

Autoconfiguring the interfaces

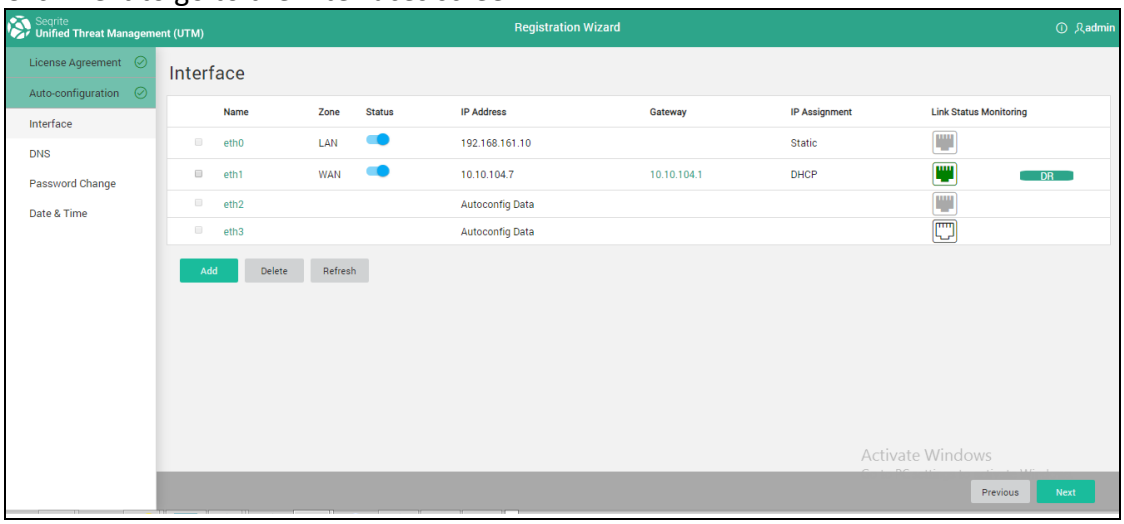
1. Click **Allow** to allow UTM to detect the networks.
2. Select the option for Interface Autoconfiguration.
3. Select the time interval for the autodetect process.
   Note: You can enter a duration of maximum 10 seconds. You have to wait for the configured duration while the autoconfiguration process is underway.



4. After the autoconfiguration process completes, the interfaces are automatically applied the settings as per the detected IP networks.

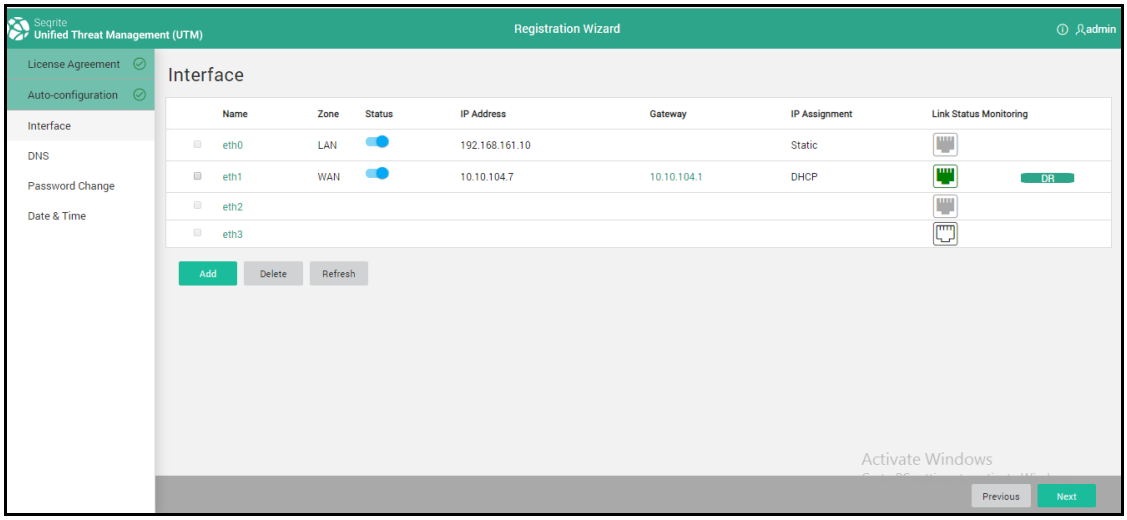


5. Click Next to go to the Interfaces screen.



6. You can either accept the autoconfigured settings or edit the interface settings as required. Click **Next** to continue.

Configuring the interfaces manually

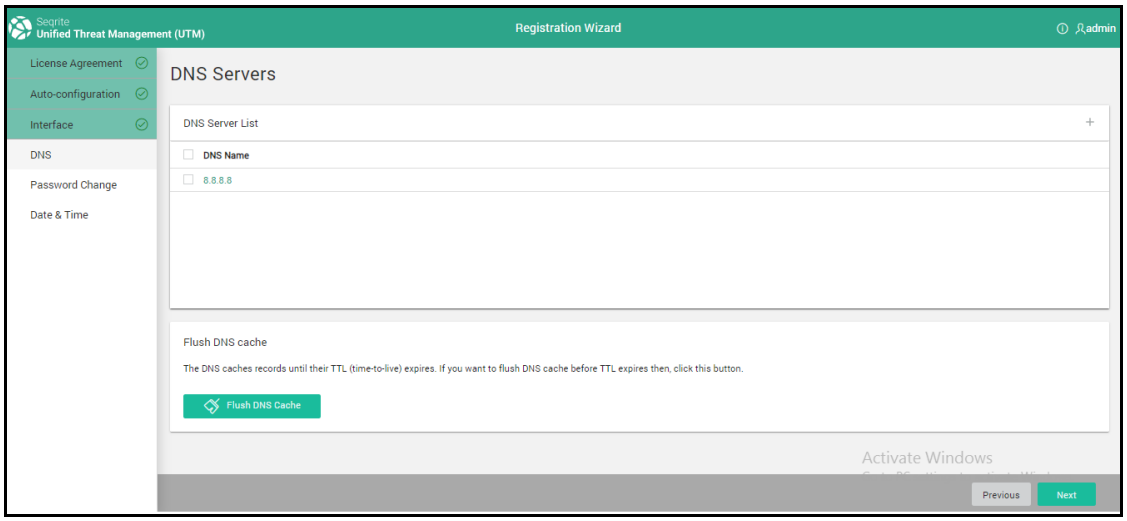


1. Click the name of the interface such as eth0 for LAN, eth1 for WAN to edit the interface settings.
2. Enter the **Interface Name** and select the **Zone** and **IP Assignment**. For LAN interface, the IP Assignment will be only Static while for WAN it can be any of the three that is Static, PPPoE, or DHCP.
3. Click **Apply** to save the changes.
4. You can also Add Interfaces, Alias, VLAN, Bridge and Link Aggregation. Click on Add to add a new interface. (For more details on Adding an interface, see Interface section.)
5. Click **Next** to go to the next step that is DNS configuration.

Configuring the DNS

This step allows you to override the default Domain Name Server settings. You can enter the DNS provided by the ISP, or the DNS that you want to use. After selecting the DNS that you want to use, you can also change the DNS priority by using the arrow buttons, which allows you to try another DNS server if the current server is down.

Registration Wizard

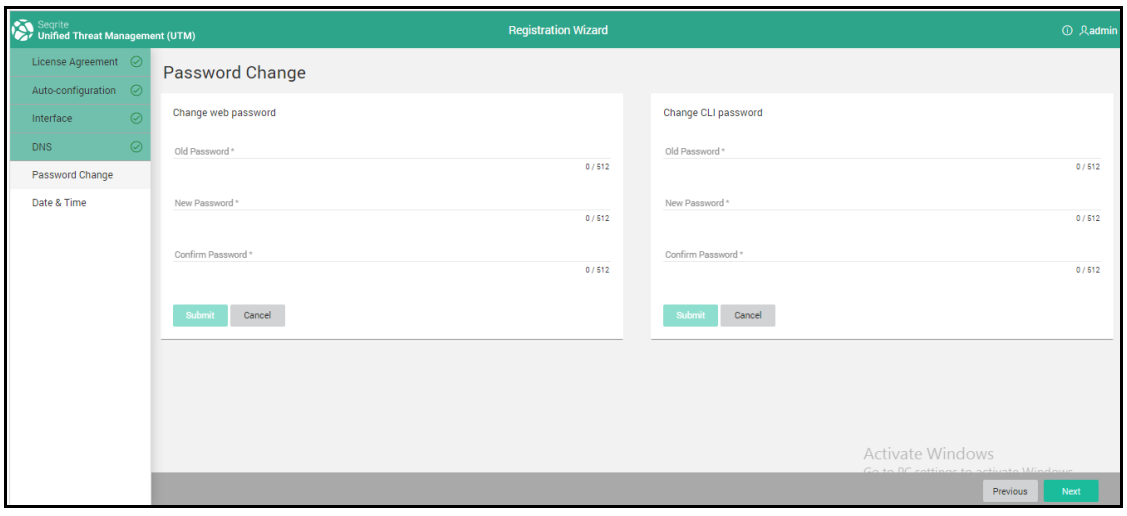


1. Click the + (**Add)** icon to add a DNS server.
2. Enter **DNS Name, IP address** in the corresponding fields and click **Save**. The DNS is added in the list.
3. Click **Next**.

Note: The DNS list cannot be blank. There should be at least one DNS entry. There will be a default entry present i.e., 8.8.8.8.

Changing the Password

You must change the default appliance password for web and CLI interface. The default password for both web console and CLI access is admin@123. On clicking the **Next** button in the DNS configuration screen, the Password Change screen is displayed.

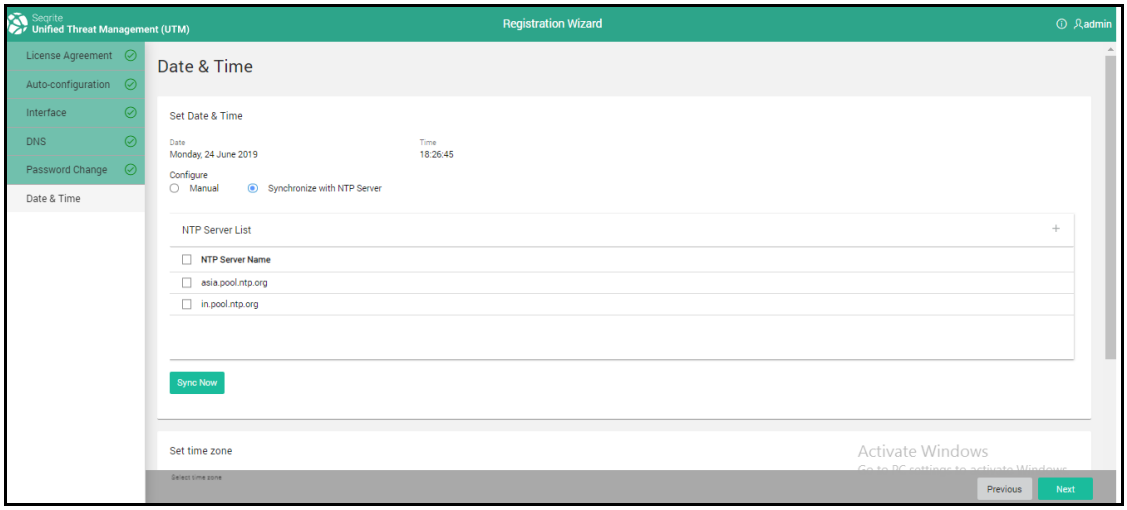


1. Enter the old (default) password for accessing Web interface, enter new password, confirm password and click **Submit**. The new password is saved.

2. Enter the old (default) password for accessing CLI interface, enter new password, confirm password and click **Submit**. The new password is saved.
3. Next time you log in to the Web or CLI interface of Seqrite UTM use the new password.

Changing the date and time

After changing the password, you need to configure the date and time on the Seqrite UTM. On clicking **Next** on the Password Change screen, the Date and Time screen is displayed. The Date and Time screen displays the current date and time of the appliance and allows you to configure the Date and Time as per different geographical regions. You can also synchronize the Date and time from an NTP server.

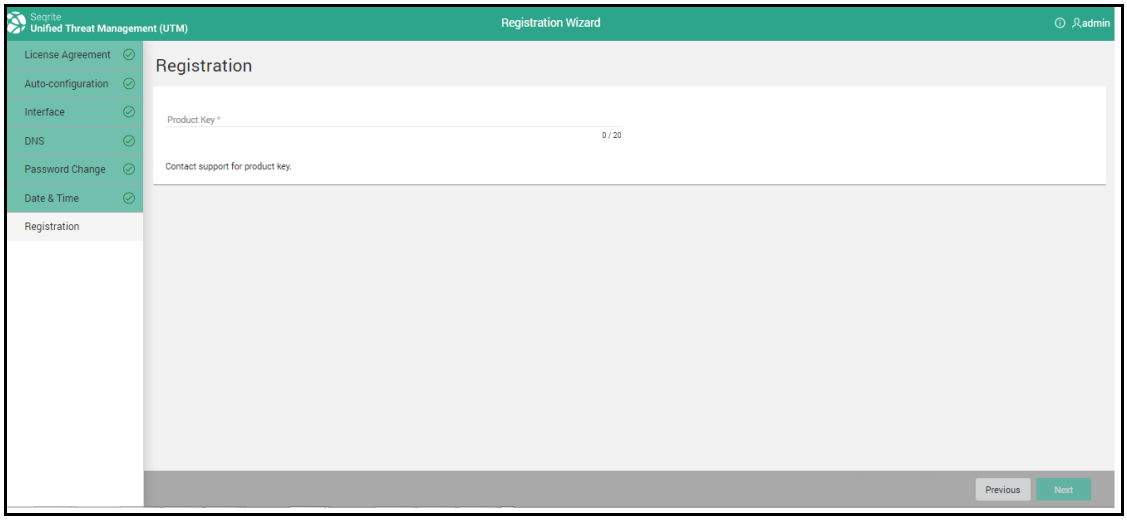


1. You can set **Date & Time** using one of the following two ways:
   I. **Manual**: Select this option to set the date and time using the date and time pickers or
   II. **Synchronize with NTP server**: Select this option to synchronize the appliance time automatically with a predefined NTP servers (asia.pool.ntp.org & in.pool.ntp.org) or add a new NTP server.

   Click **Sync Now** to sync appliance clock with the listed NTP servers. The time will be synchronized with the NTP server having least time difference.
2. Select the **Time Zone** according to the geographical region in which the appliance is deployed.
3. Select the time format, date format, and the first working day of the week.
4. Click **Save** to save the changes.
5. Click **Next**. The Product Key screen is displayed.

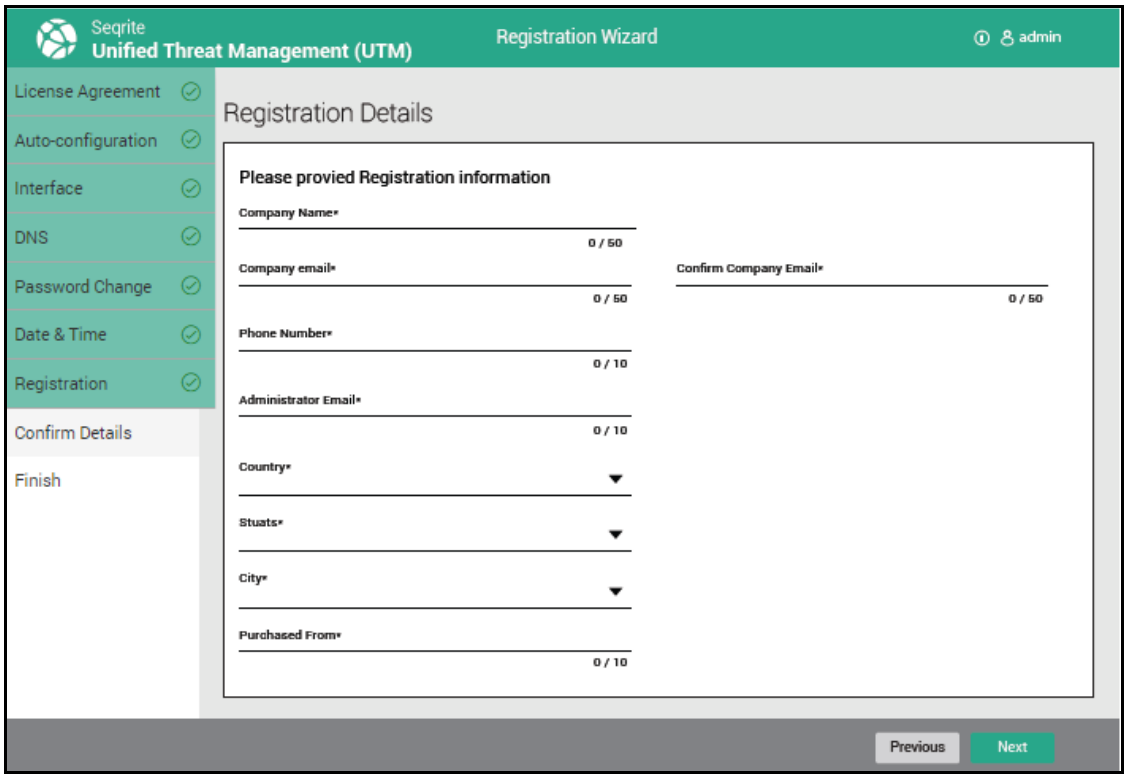
Registering the product (Online)

You need a working Internet connection for the registration process. While registering the Seqrite UTM appliance you need to provide the Product key of your appliance. On clicking Next on the Date and Time setting screen, the Registration Product Key screen is displayed.



1. Enter a valid Product Key and click **Next**. The product key is given to you on purchase of the Seqrite UTM appliance. If you have not got the product key, contact your Seqrite sales representative.

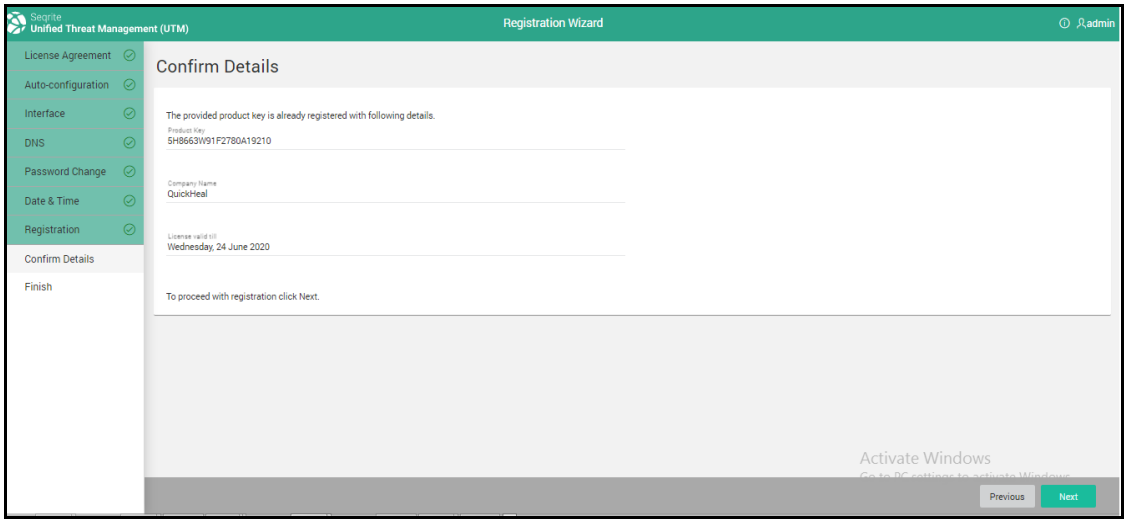
   In case of new appliance registration, the Registration Details screen is displayed.



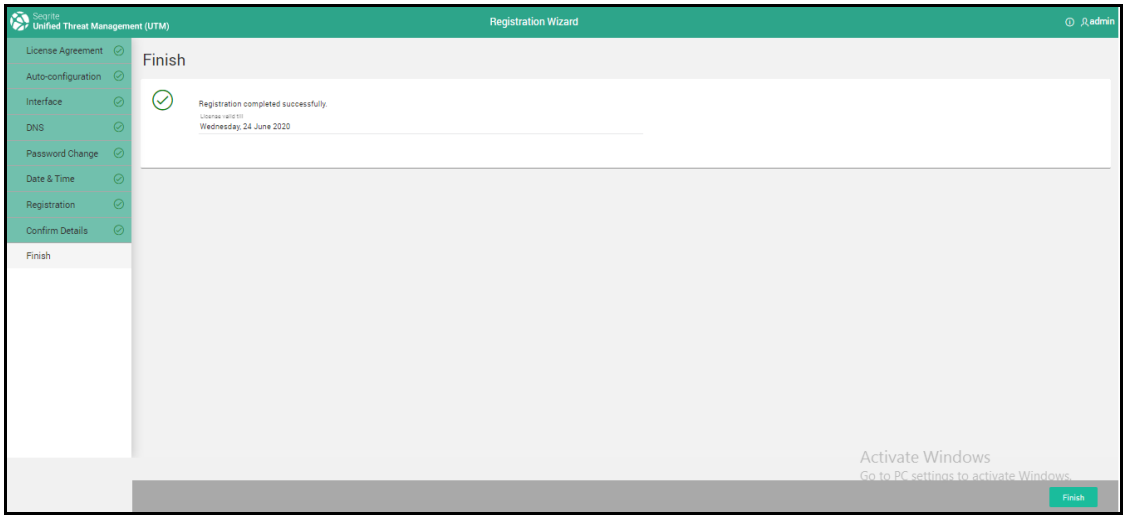
2. Enter the required details and click **Next**.

   Note: Fields marked with red asterisk are mandatory.

3. Click **Next**, the Confirm Details screen is displayed.

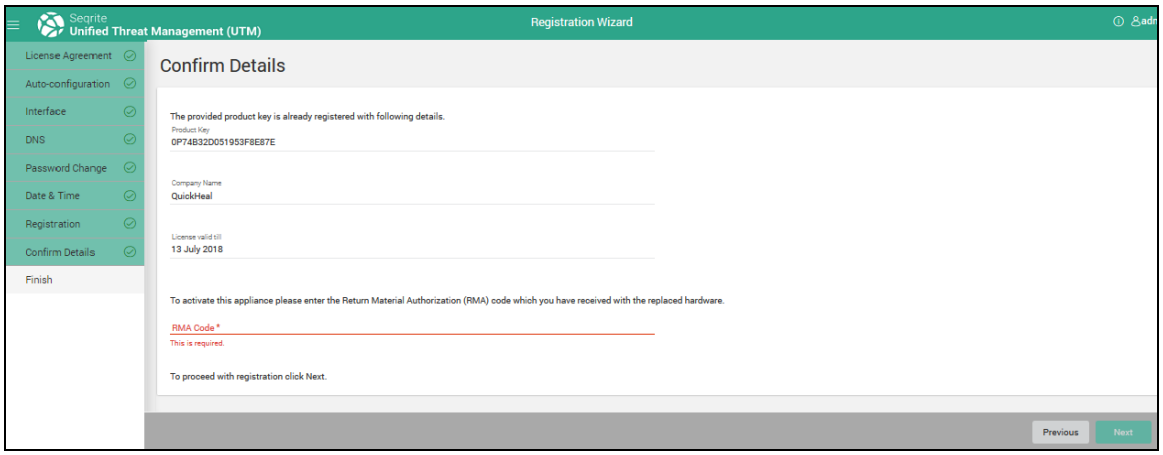


If you upgrade Seqrite UTM to the latest version or in case your organization faces certain specific issues you need to perform reactivation of the appliance. In case of reactivation the following screen is displayed, after entering the Product Key.

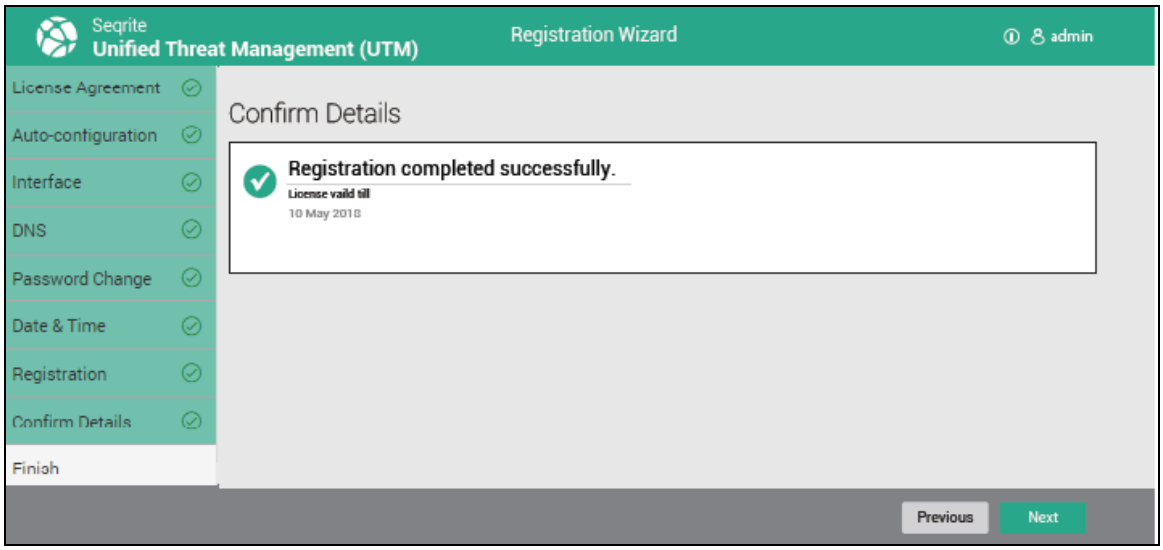


4. Confirm the details and click **Finish**.
5. In case of a hardware replacement you need to provide the Return Material Authorization (RMA) code during registration. You receive the RMA code with the replaced hardware. In this case the following screen is displayed.

Registration Wizard



6. Enter the **RMA code** and click **Next**. On successful registration, the License Validity screen is displayed.



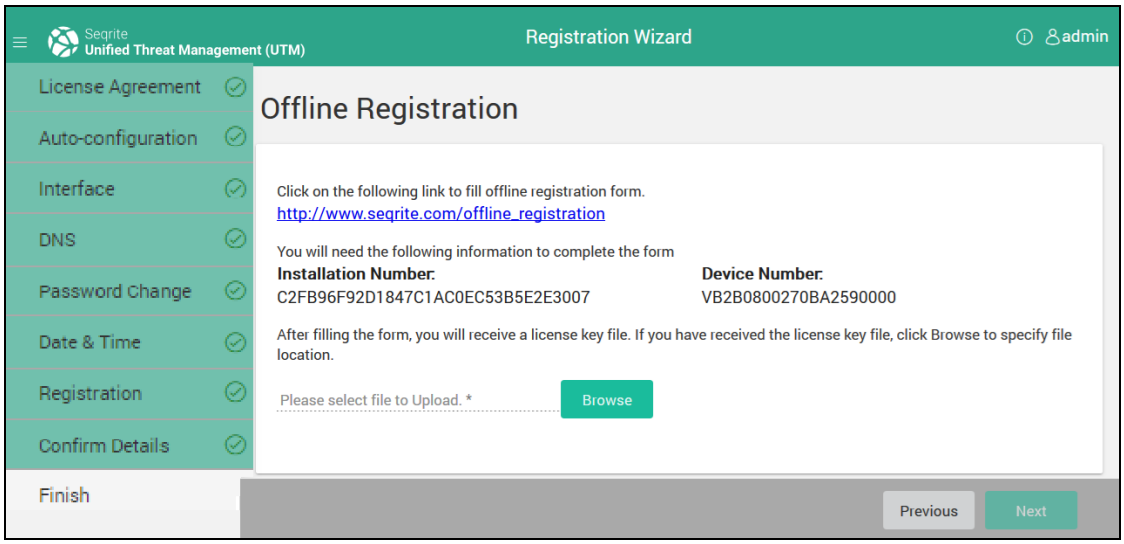
7. Click **Finish**, to finish the registration process of the appliance. On clicking **Finish**, you will be logged out. Ensure that you use the new password for any subsequent login attempts.

   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.

Offline registration

If an Internet connection is not available, you can register your Seqrite UTM appliance offline also. You will need the product key to perform offline registration:

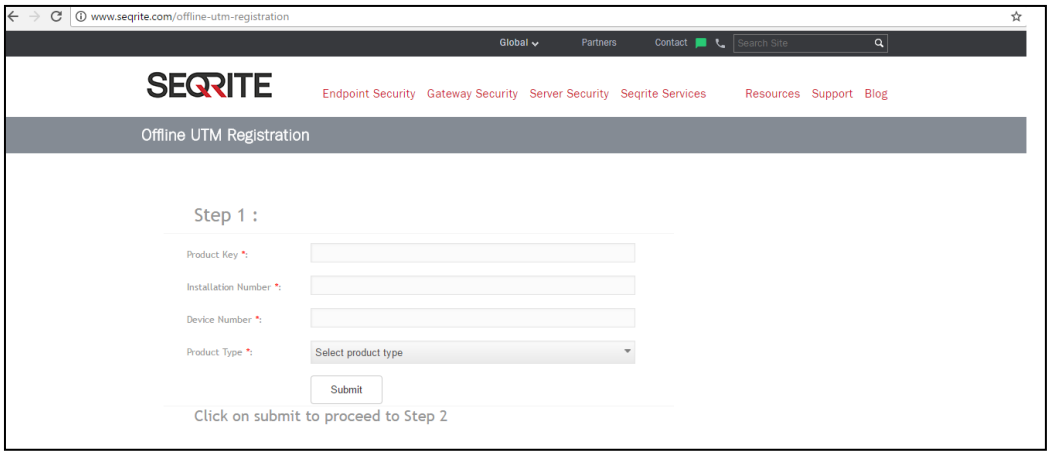
Registration Wizard



1. Click **Registration**. If Internet connection is not available, click **Next** to register offline. The Offline registration screen is displayed.

The link for Offline registration is displayed. If an Internet connection is not available, you can copy and save the link for use later.

2. Copy the Installation Number that is generated on the earlier screen.
3. On a computer that has an Internet connection, click the link http://www.seqrite.com/offline_registration.
4. Click the link for the Seqrite UTM. The offline Registration form is displayed.



5. Enter the product key, the Installation number and device number generated in the earlier step, select your product type as Seqrite UTM, and click **Submit**. The license key file is downloaded on your computer.
6. Copy the license key on your appliance/computer and click **Browse** to select and upload the license key file.

7. Click **Next.** The license key file will be authenticated, and your appliance will be successfully registered.
8. Click **Finish**.

Chapter

3

Accessing Seqrite UTM

Seqrite realizes the varying network setup in different organizations and has provided installation recommendation for three prominent network setups. For more details on network setup and registration of Seqrite UTM you can refer the Seqrite UTM Getting Started Guide.

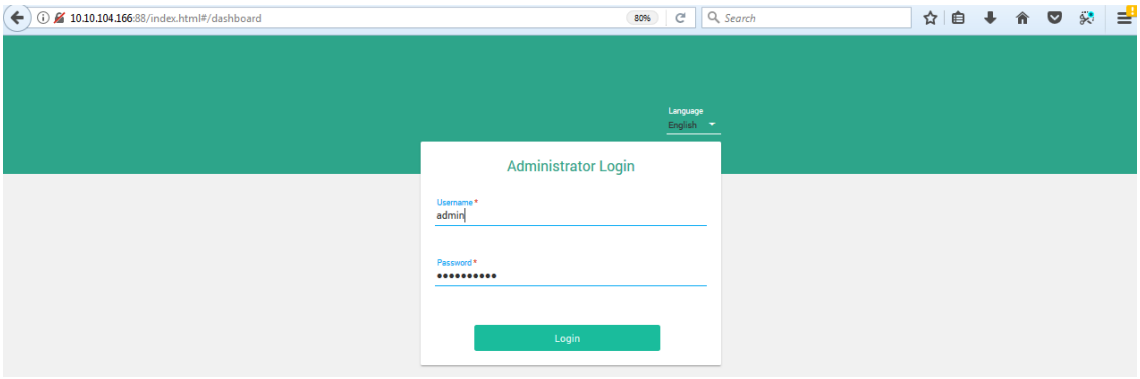
Logging on to Seqrite UTM

You can use the following two ways to access Seqrite UTM:

- Accessing Seqrite UTM through Web
- Accessing Seqrite UTM through CLI

Accessing Seqrite UTM through Web

1. Launch the web browser and enter the IP address of the Seqrite UTM appliance in the address bar. The login page is displayed.



2. Enter your **Username** and **Password** in the designated text boxes.
3. Click **Login**, the Home page is displayed.

Accessing Seqrite UTM through Command Line Interface (CLI)

Apart from using the web interface to logon to Seqrite UTM, you can logon to Seqrite UTM using the Command Line Interface (CLI) using a terminal emulator or client such as PuTTy. The CLI console provides a collection of tools that helps to administer, monitor, and control certain Seqrite UTM components.

You can access Seqrite UTM CLI console in the following two ways using the below mentioned default credentials:

Username: admin

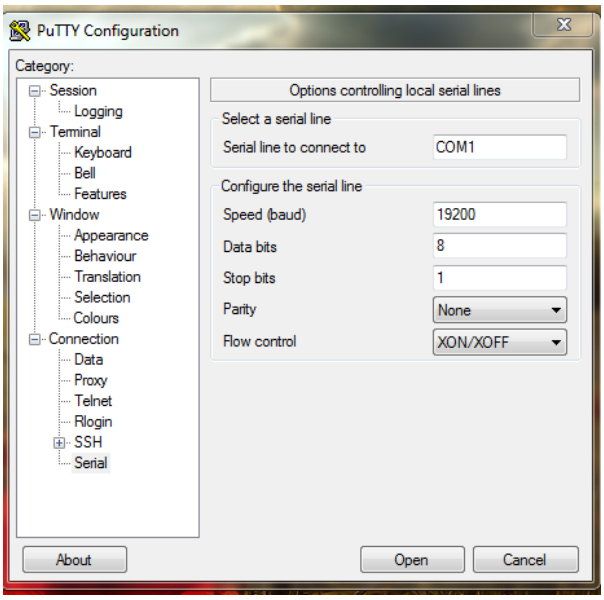
Password: admin@123

- **Direct connection**: You can connect a keyboard and monitor directly to Seqrite UTM using VGA or a console cable, i.e. the com port.

  When you connect to Seqrite UTM using VGA, the boot device should be SATA:3M San-Disk SDCFH-003G.

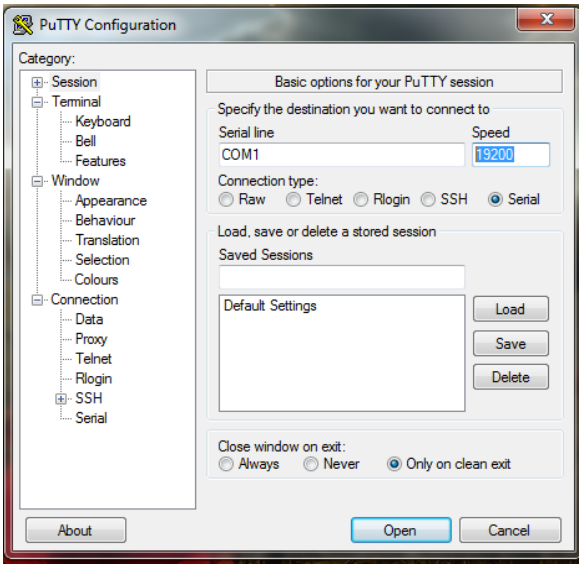
  When you connect to Seqrite UTM using a console cable, make the following settings in PuTTy, to access CLI.

  1. Set the speed baud rate as 19200. Note: Baud Rate can be set at 115200 for some machines.



  2. Select the Connection type as Serial, as shown below:

Accessing Seqrite UTM



- **Remote connection**: You can remotely connect to Seqrite UTM in the following ways:

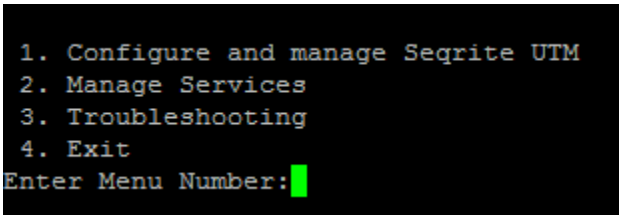
    1. Accessing CLI console via remote login utility such as Telnet. Telnet xxx.xxx.xxx.xxx where xxx.xxx.xxx.xxx is the IP address of Seqrite UTM.

        Note: Telnet is disabled by default.

    2. You can access Seqrite UTM CLI console using SSH client.

        Note: SSHv1 and SSHv2 both are supported.

- On successful login, the following Main Menu screen will be shown:



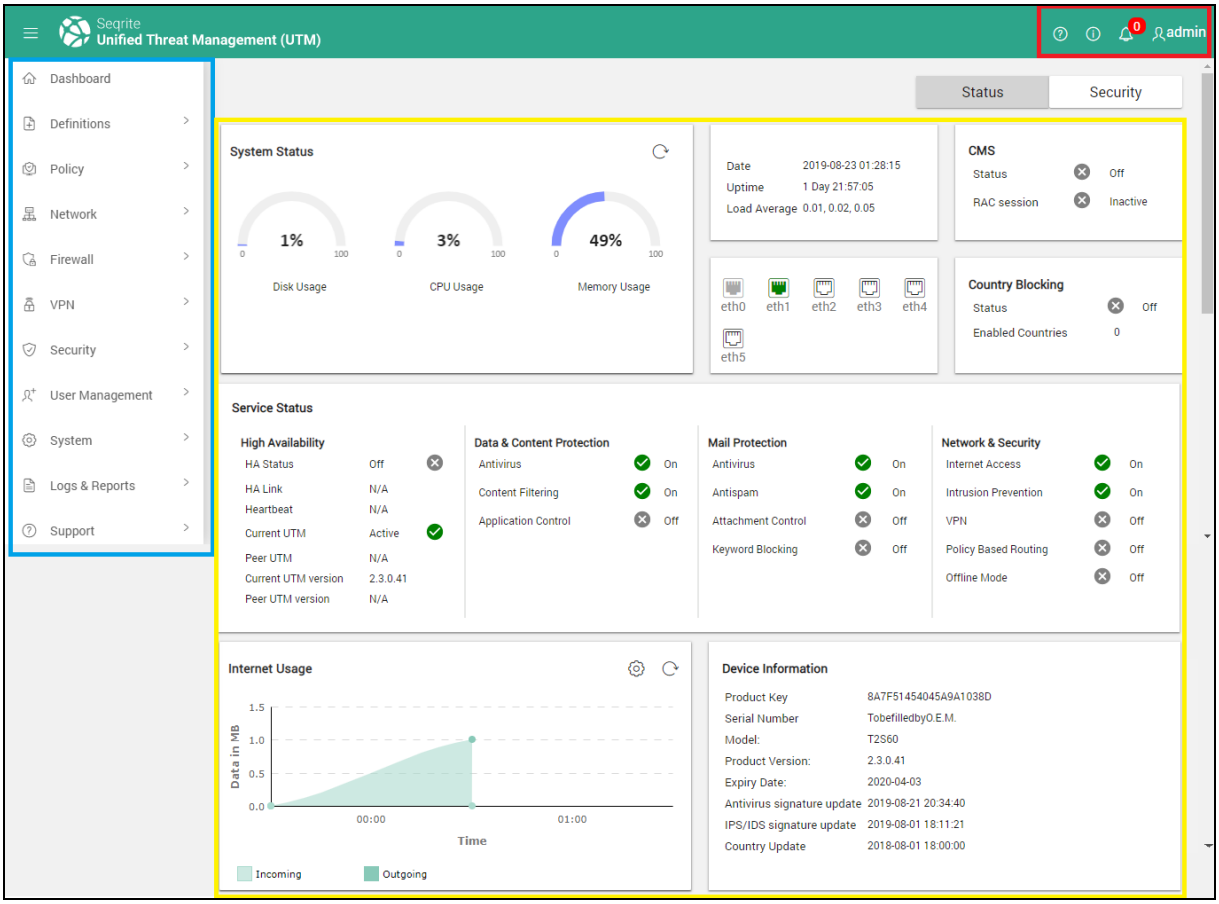
To access any of the menu items, type the number corresponding to the menu item against **Enter Menu Number** prompt and press **Enter**. Every submenu has a **Previous** and **Exit** option. Use '**Previous**' to go one level up and '**Exit**' to exit from CLI console.

Before registration you can access only the following menus through CLI:

- **Configure and Manage Seqrite UTM**: Helps you to reset web Super Administrator password, configure interfaces & DNS, reboot and shut down the Seqrite UTM appliance.
- **Manage Services**: Lets you manage the various services. For more information, see Command Line Interface.
- **Troubleshooting**: Helps you to Ping & Traceroute IP and run diagnostic tests on the Seqrite UTM.

Navigating through Seqrite UTM (Web console)

Navigating through the Seqrite UTM web console is easy and intuitive. The console is divided into three main user areas, one on the upper right section for console related administrative functions (highlighted in red), the left pane (highlighted in blue) that has expanding nodes for functional options, and the dashboard or main action area (denoted in yellow) which displays the current selected activity and related screens.



The upper right section (highlighted in red) is always available from any of the pages and has the following options:

Tab	Function
Help	**Help** – Provides a set of help files which guides you to use Seqrite UTM.
Diagnostics & Contact Us	**Diagnostics –** To help you with diagnosing the issues with Seqrite UTM. **Contact Us** – For accessing the available support options to contact Seqrite.
Notifications	Displays the notifications related to license expiry, antivirus updates, status, disk space, and other critical notifications. For more information

Tab	Function
	on notification messages, see Notifications.
Admin Options	**Reset CLI password** – To reset the CLI password. The CLI can be accessed only by super administrator user. Click this option and enter the new password and confirm the password. Click **Submit** and the CLI password is changed.
	SSL certificate – Click option to download SSL certificate in .pem format.
	Shut down – Click option to power down the Seqrite UTM appliance.
	Reboot - Click option to restart Seqrite UTM.
	Change web password - Use Change Web Password to change the password of the currently logged in administrator. On clicking this the following options are displayed: 1. **Old Password**: Provide the current password of the logged in administrator. 2. **New Password**: Provide the new password which should be set. 3. **Confirm Password**: Re-enter the new password. 4. Click **Submit**, the password is changed, and administrator is logged out. On subsequent logon, administrator should logon with new password. Note: Even if you change the Web password of super administrator the CLI password is not changed.
	Logout - To logout of the Seqrite UTM web console.

Notifications

The following table lists the possible notifications and the associated scenarios:

Notification	Description
Licensed user capacity is exceeded. Upgrade the license to support more users.	This notification is displayed when the number of users currently logged in to Seqrite UTM are more than or equal to the licensed users limit.
Update service is not running. Please	This notification is displayed when the Antivirus database update service has stopped running.

Notification	Description
contact technical support.	
Antivirus protection is out of date.	This notification is displayed when the Antivirus is not updated for more than 3 days. Use **Update Now** button to update the Antivirus protection.
Seqrite UTM License is about to expire. Please renew your license.	This notification is displayed when a license is about to expire. It alerts the administrator to renew the license of Seqrite UTM. The alert starts from 30 days before the license is to expire.
Your disk space is almost full. You are requested to export the existing reports before they get deleted by the system.	This notification is displayed when the disk is more than 85% full. Administrators are requested to download the reports as a cleanup activity. The system will delete the oldest reports first and then the oldest logs to make disk space available.
Seqrite UTM license has expired. Please renew your license.	This notification is displayed when the Seqrite UTM license has already expired. When the Seqrite UTM License expires the Antivirus Update and Web site categorization services are stopped. After the license is renewed these services are resumed.
IPS service has been disabled due to some technical problem. Please contact technical support.	This notification is displayed when IPS service is not able to start due to some technical problem.
IPS update is available. Do you want to update now?	This notification is displayed when IPS Update is available. IPS rule Update check is scheduled after every 12 hours.
Your log size is about to reach the limit. You are requested to export the existing logs before they get deleted by the system.	This notification is displayed when the size of log files in Archive has reached 30 MB. Logs are deleted from the archive if the logs reach the limit. The oldest log is deleted first.

Notification	Description
Your license is blocked. You will not receive updates. Please contact customer support.	This notification is displayed when the license is blocked as multiple devices are using same product key.
Country-to-IP database update has started	This notification is displayed when update process for updating Country-to-IP database has started.
Country-to-IP database update has failed	This notification is displayed if update process for updating Country-to-IP database has started and then failed due to some issues.
CMS Registration failed due to expired UTM license	This notification is displayed when admin tries to register UTM appliance to the CMS portal and the process failed because the UTM license has expired.
UTM appliance failed to register with CMS.	This notification is displayed when admin tries to register UTM appliance to the CMS portal and the process fails because of some connectivity issue, or if the CMS portal doesn't respond or an issue with .dat file required for registration.
UTM appliance successfully registered with CMS	This notification is displayed after the CMS portal successfully registers the UTM appliance.

Features

The Features pane (highlighted in blue) has the various functional options grouped in respective categories as described in the following table:

Dashboard	Displays the real-time information of services, the interfaces, system, and device information of Seqrite UTM.
Definitions	Lets you create/modify/delete definitions for network, service, and file. These definitions can be reused any number of times during configurations.
Policy	Lets you create policies for Time category, URL categorization, File size blocking, Keyword Blocking, and define Internet Quota, Time quota, Device Quota, and Bandwidth control.
Network	Lets you manage the interfaces, IPv6 settings, DNS servers, configure the DHCP server, configure the Proxy server, create routes that are based on policy, multicast, and static

	types. You can also configure Seqrite UTM interfaces for load balancing.
Firewall	Lets you configure the default, Interzone, Custom and forwarding rules for firewall.
VPN	Lets you configure the VPN server based on IPSec, PPTP, SSL, and the associated clients.
Security	Lets you configure the settings for IPS, Antivirus, Mail protection, and application control.
User Management	Lets you manage users, groups, Guest users, and Authentication server.
System	Lets you configure the date and time, administrative options, customize the portal, tweak the various settings, and configure notification settings. You can also carry out a factory reset on Seqrite UTM, backup and restore, view and manage certificates and license information, configure services for offline mode, perform firmware upgrades manually, view and manage service and system updates.
Logs and Reports	Lets you view the reports for Internet traffic, security protection, update logs, event logs and view and purge settings for logs.
Support	Lets you check the availability of a particular host and use the port mirroring option for diagnostics. You can also view the available support options to contact Seqrite helpdesk.

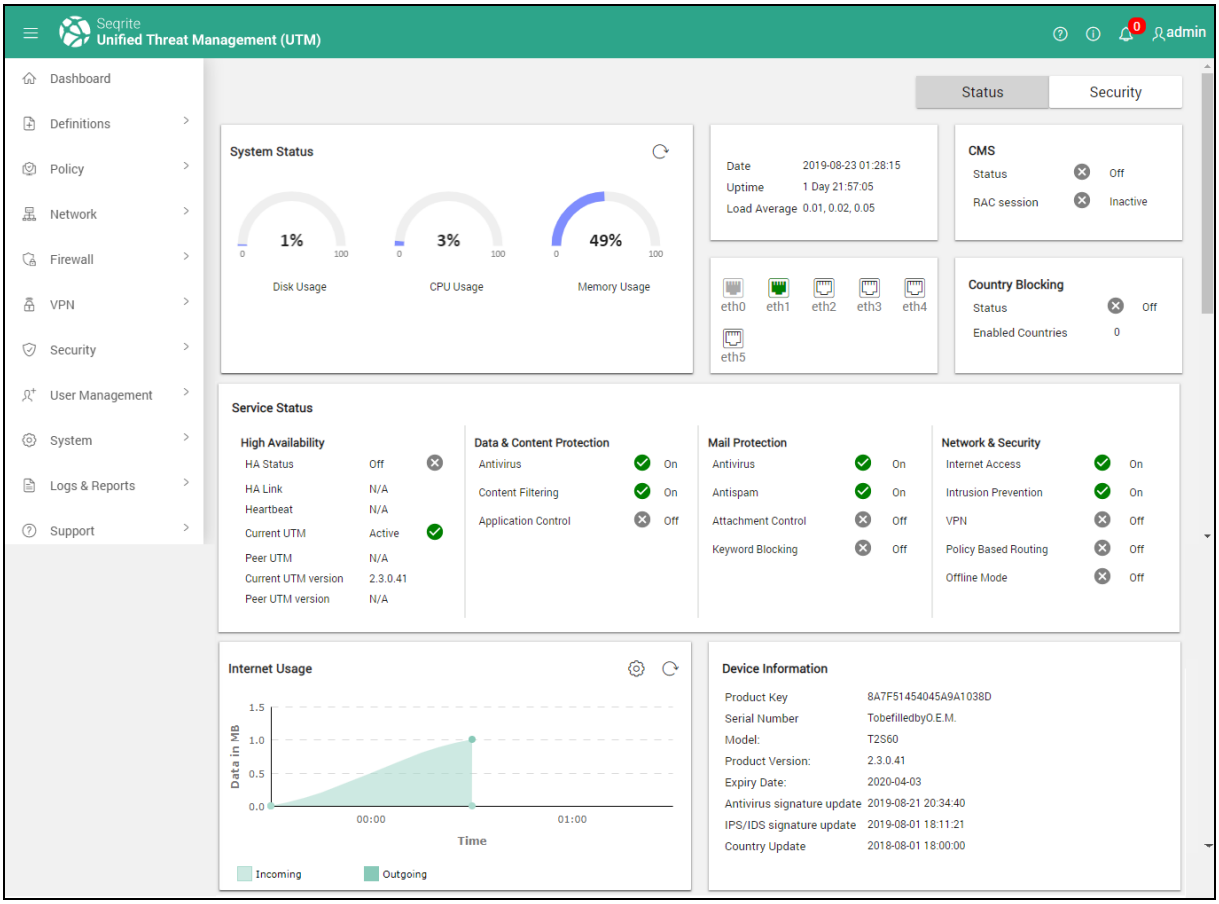
Chapter

4

Dashboard

The dashboard or the main action area is the first page that is displayed when you logon to Seqrite UTM. The dashboard has two views that can be selected by clicking the Status or Security tabs on the upper right corner. The dashboard displays the real-time status of the various activities carried out by Seqrite UTM.

Dashboard – Status tab



The dashboard for Status tab displays the following widgets and information:

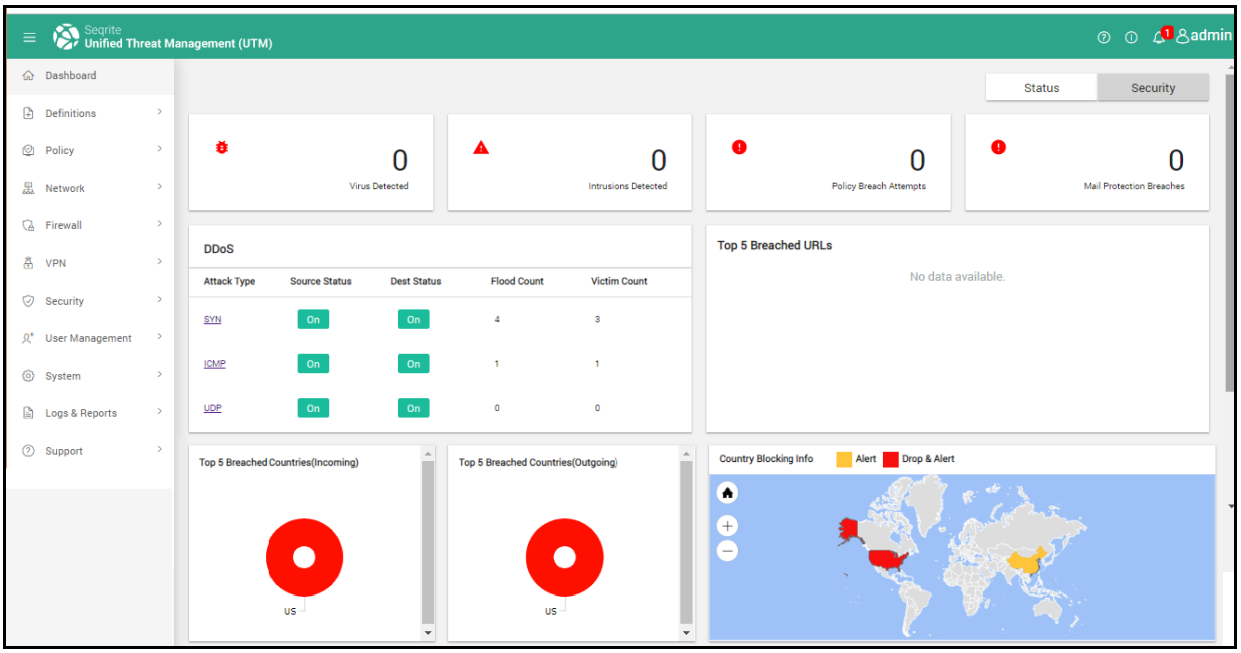
Dashboard

- System Status: Displays the disk, CPU, and memory usage, apart from the System Date and time, and the Uptime for Seqrite UTM. Click the refresh icon for latest information on system status.
- Interface Status: Displays the status for the connection interfaces, eth0, eth1, eth2, etc. available on Seqrite UTM.
  Interfaces status and description

Icon	Description
	Indicates that Ethernet cable is connected.
	Indicates that the Ethernet cable is connected & Internet is available.
	Indicates that the Ethernet cable is connected & Internet is not available.
	Indicates that Ethernet cable is not connected.
	Indicates that WLAN or WIFI is available for connecting. Applicable only for the NGS130W model.

- CMS status: Displays status for CMS support whether enabled and RAC session if any active.
- Country Blocking: Displays the status for the country-based blocking feature whether enabled or disabled and count for countries enabled.
- Service status: Displays the service status and information for the following:
  1. High availability whether enabled or disabled.
  2. Data and content protection: Displays the status of Antivirus, content filtering, and application control whether enabled or disabled.
  3. Mail Protection: Displays the status for antivirus, antispam, attachment control, Keyword blocking and DLP feature whether enabled or disabled.
  4. Internet and networks: Displays whether Internet access, Intrusion Protection, VPN, Policy based routing and Offline modes whether enabled or disabled.
- Internet Usage: Displays the incoming and outgoing data usage with time for the selected interfaces. Click on the incoming and outgoing usage boxes to enable or disable as required.
- Device Information: Displays the product key, model name, product version, license validity, and Antivirus, IPS/IDS signature last update.

Dashboard – Security Tab



The dashboard for the Security tab displays the following widgets and information:

- Count of viruses detected: Click tab to view report of viruses detected and blocked in the network and the name of the user who handled the infected files.
- Intrusions detected: Click tab to view a detailed report of the intrusions and source IP of the intrusions.
- Policy breach attempts: Click tab to view a list of websites that have been visited in breach of policies, their category and the name of the user causing the breach.
- Mail Protection breach: Click Tab to view report for mail breaches as required.
- DDoS status: Displays the status for DDos protection for the SYN, ICMP, and UDP protocols whether enabled or disabled and the corresponding flood and victim count for each.
- Top 5 Breached URLs: Displays the list of the top 5 blocked URLS that users have tried to access.
- Top 5 Breached Countries: Displays the count for breaches for country-based traffic blocking if enabled. There are separate widgets for incoming and outgoing traffic for the breaches that occurred.
- Country blocking info: Displays a pictorial representation of world map, that can be zoomed in or zoomed out for viewing countries for which country-based blocking is enabled. The configured action whether to alert or alert and drop is also displayed by yellow and red colors respectively.

Chapter

5

Definitions

Definitions are predefined network traffic types and services which can be reused while configuring various Seqrite UTM modules. Seqrite UTM allows you to add the following types of definitions:

MAC: You can now create a definition of single MAC address or a list of MAC addresses. This definition can be used in custom firewall rules and proxy settings.

Network: Helps you to define / add an entire network subnet.

Service: Helps you to add protocols and ports used by an application for communication.

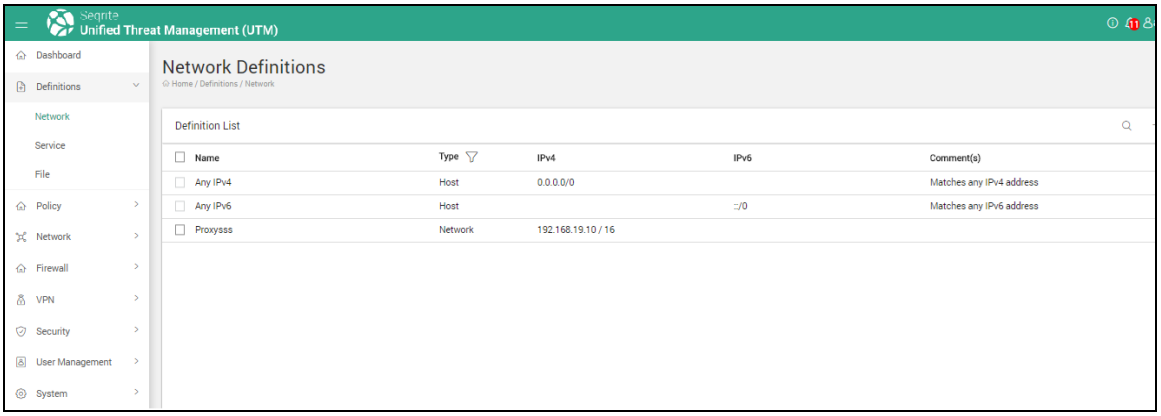
File: Helps you to define file extensions that can be used in mail protection attachment control and content filtering.

FQDN: Helps you define Fully Qualified Domain Names definitions that you can use to allow or block as per policy.

Time category: Helps you define the various time categories that you can apply to the users and groups for restricting the time for Internet access.

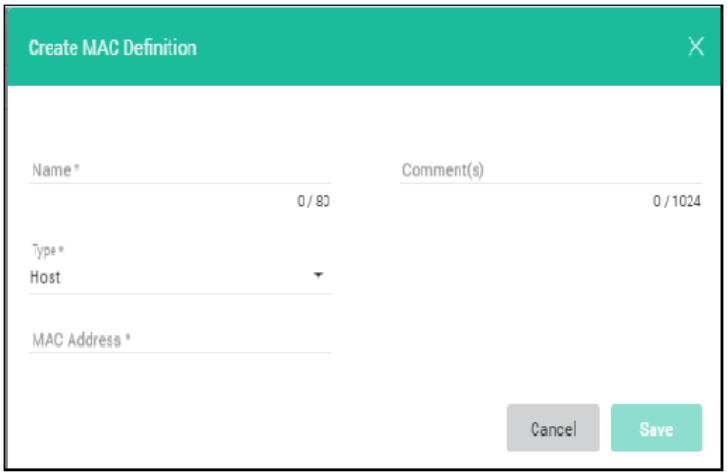
Custom URL Category: Create categories of URLS that can be allowed or blocked while creating the URL categorization policies.

The Definitions page displays list of networks definition and services definition. You can search definitions by Name. You can also add, edit, or delete the definitions.



Adding MAC definition

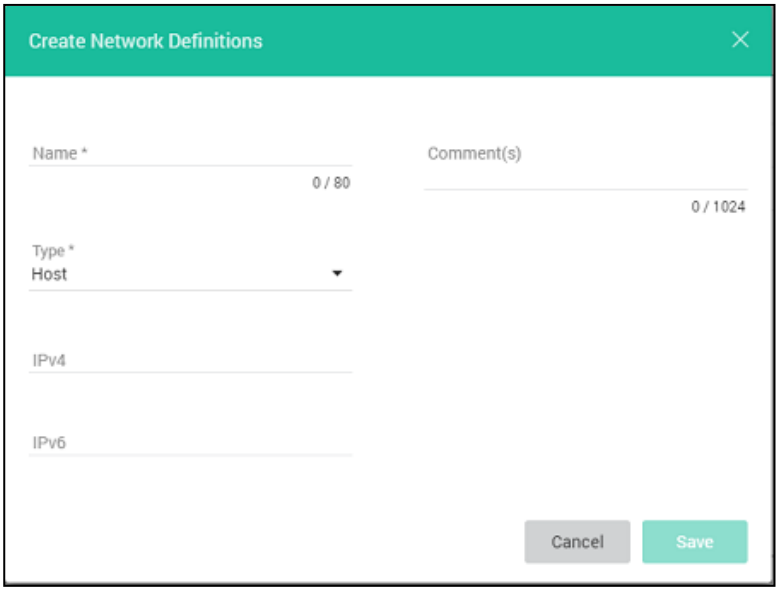
1. Navigate to Definitions > MAC.
2. Click + to add a new MAC definition.



3. Enter the name for the definition and related comments.
4. In the Type drop-down list, select whether the entry is for a host or for a list of MAC addresses. You can select host for a single MAC address or use the list option to add multiple MAC addresses. When using the list option, enter the multiple MAC addresses separated by a comma.
5. Click **Save**.

Adding Network Definition

1. Navigate to **Definition > Network**. The following page is displayed:
2. Click + (**Add)**. The Add Network Definition dialog box is displayed.



3. Enter the definition name in the designated text box and add the relevant description in the comments text box.
4. Select the Network Definition type from the drop-down list that is displayed. The Network definitions are of the following four types:

    i. **Host**: Allows you to define single IP address. Enter the IPv4 / IPv6 address.

    ii. **IP Range**: Allows you to define the range of IP addresses. Enter IPv4 /IPv6 address range as applicable.

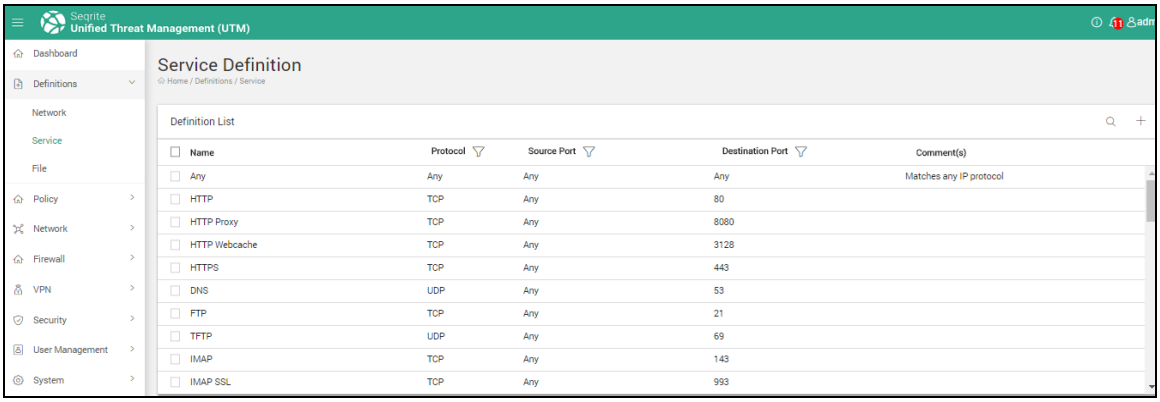
    iii. **IP List**: Allows you to define a random list of IP address. Enter IPv4 / IPv6 IP addresses separated by a comma. For e.g. 192.168.10.10, 202.212.34.56,212.25.34.56

    iv. **Network**: Allows you to define a network containing a set of IP addresses. Enter IPv4 network address and select subnet mask from drop-down values. For IPv6 enter IPv6 network address and IPv6 prefix value.

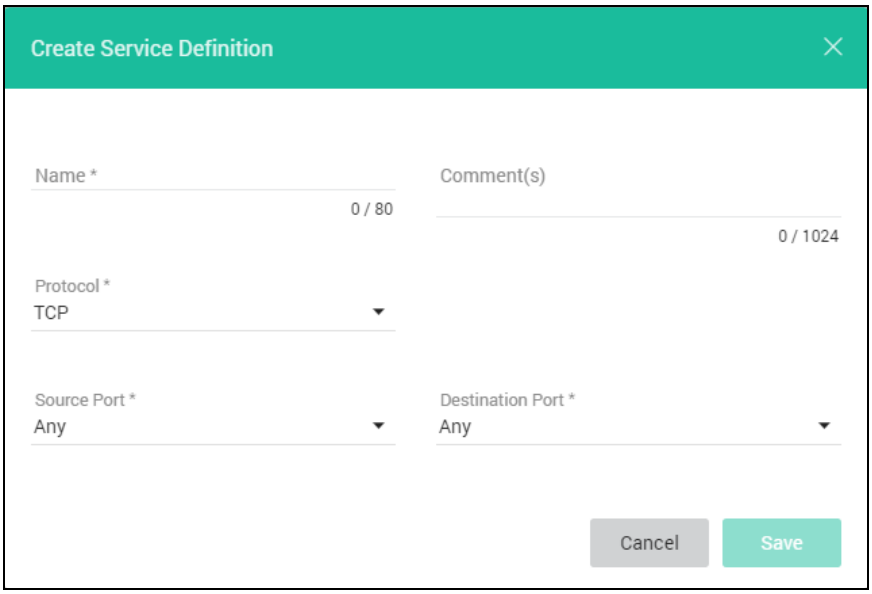
5. Click **Save**. The newly added Network definition is displayed in the list on the Network Definitions page.

Adding Service definitions

1. Navigate to **Definition > Service.** The following page is displayed.



2. Click + (**Add)**. The Create Service Definition dialog box is displayed.



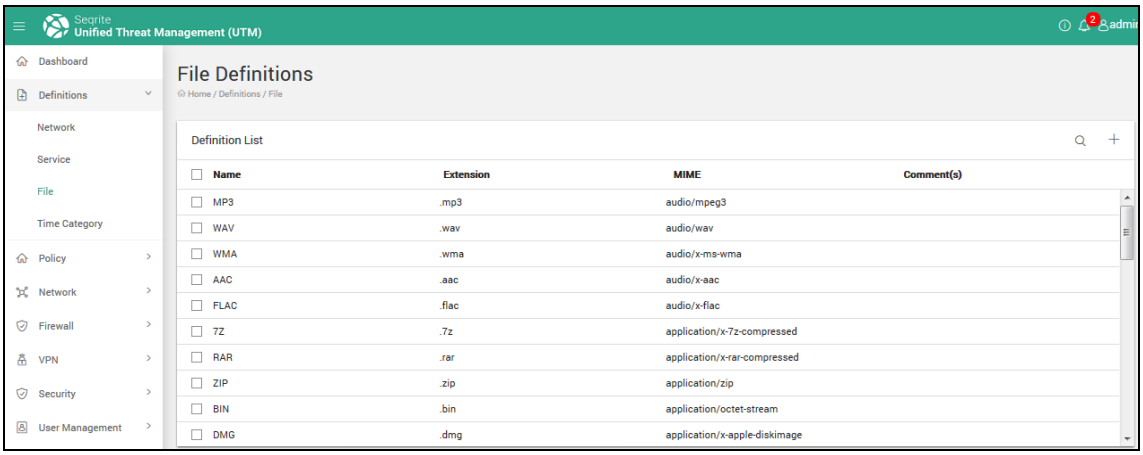
3. Enter the Service definition **Name** in designated text box and the description in comments field.
4. Select the appropriate network protocol from the drop-down list.
   Protocols are of the following 4 types:
   1. TCP
   2. UDP
   3. ICMP
   4. IGMP
5. Select the Source Port from the drop-down as applicable. This is the port where the client initiates the connection for communication.

- Any: Allows you to set any port as source port.
- Port(s): Allows you to enter a single port or a range of ports.

6. Select the Destination Port. This option is displayed when you choose Service definition Category. This is the port where the connections are accepted for communications.
   - Any: Allows you to set any port as destination port.
   - Port(s): Allows you to enter a single port or a range of ports.
7. Click **Save**. The newly added service definition is displayed in the list on the Service Definitions page.

Adding File Definitions

1. Navigate to **Definition > File**. The following page is displayed:



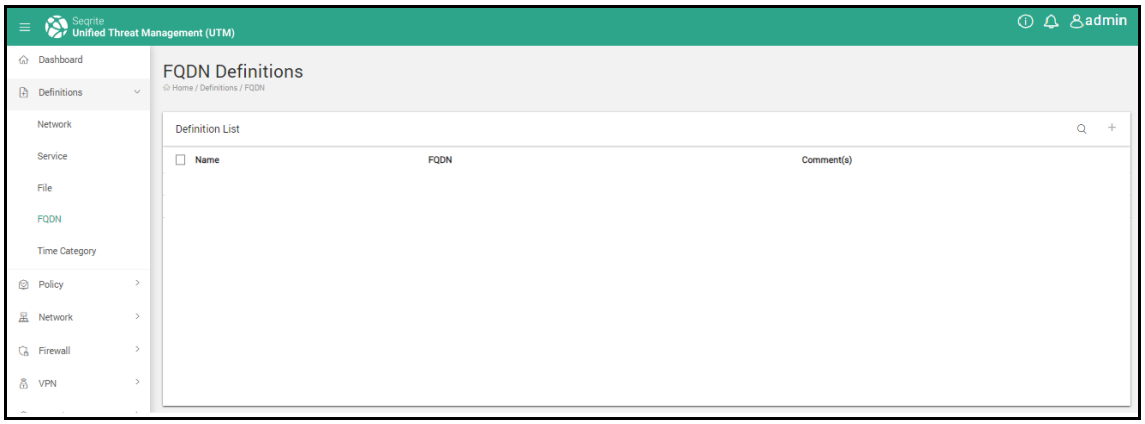
2. Click **+ (Add)** icon. The Create File Definition dialog box is displayed.
3. Enter the **File definition Name** and the description for file definition in the Comments field.
4. Enter the File extensions that you want to add to this definition. For e.g. *.docs, *.xls.
5. Click **Save**. The newly added file definition is displayed in the list on the File Definitions page.

Adding FQDN definitions

You can create a FQDN definition and add a domain name such as www.example.com to the FQDN definition list. You can use this entry from the FQDN list to allow or block access to that domain while creating a custom rule. You can also use the entries in the FQDN definition list as source while creating port forwarding rules.

Note: Wild card entry is not supported for a FQDN definition. The exact domain defined in the FQDN entry will be blocked or allowed access as per the rules where the FQDN entry is utilized. Domains resolving only to IPv4 addresses are supported under the FQDN definition list.

1. Navigate to **Definitions > FQDN**. The FQDN definitions page is displayed.



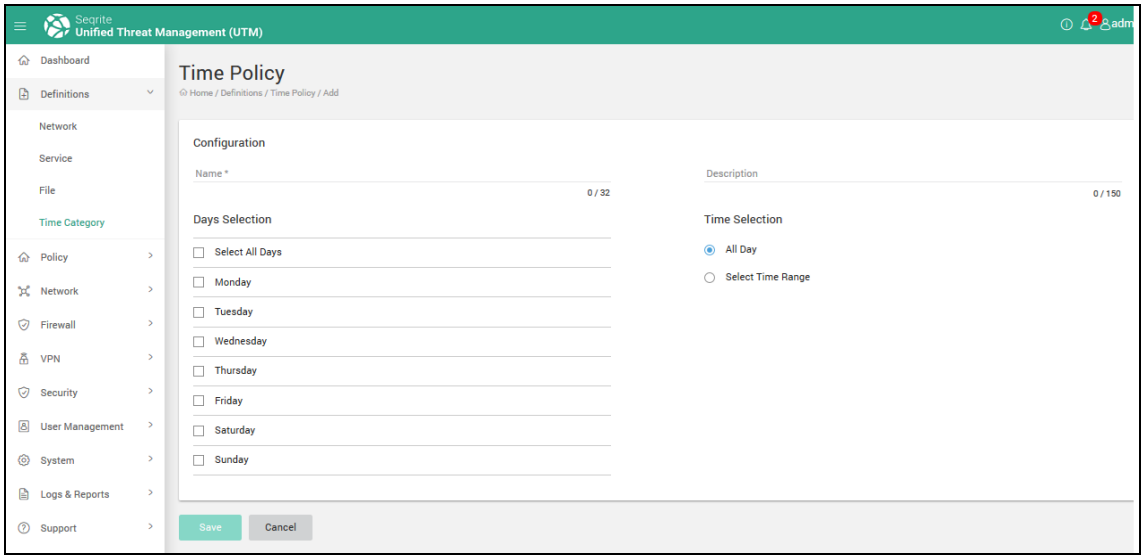
2. Click + (Add) to add a new FQDN definition.

3. Enter the name and comments if required.
4. Enter the FQDN as required.
5. Click **Save**. The entry is saved and added to the FQDN definition list.

Adding Time category

You can define certain time slots as per your requirements. These time category slots will then be applied to various users and groups. These time slots are the duration when the users can connect to the Internet.

1. Navigate to **Definitions > Time category.** The following screen is displayed.

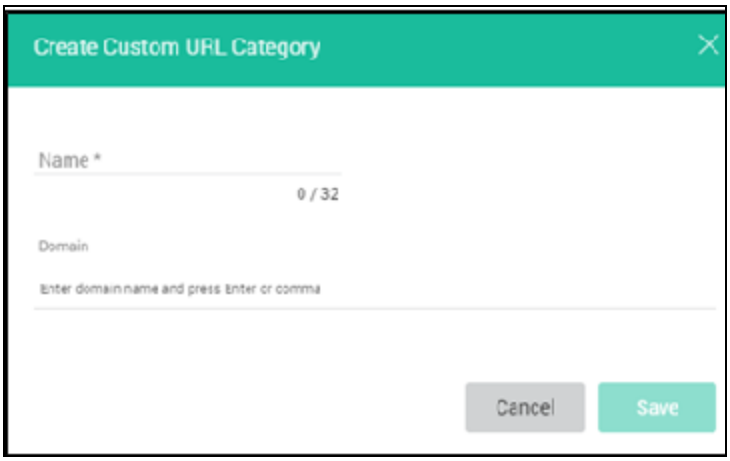


2. Click **+ (Add)** to add a new Time category.
3. Enter a name for the Time category and the description.
4. Select the days on which the category will be applicable.
5. Select the type of time slot whether all day or a specific time duration as per your requirement.
6. Click **Save**. The Time category is saved and displayed in the list.

Adding Custom URL category definition

Sometime when a category is blocked by UTM, you may need to access a particular website that falls under that category. Under the definitions section, you can create a custom URL category and under that category you can list the URLS of the websites that you want in that category. Next under Policy, in the URL Categorization, define the allow or block actions as required. This custom URL web category has higher priority than the default web category when allowing/denying the access. You can add multiple domains in a custom category and allow / block the custom category domains using the URL categorization policy.

1. Navigate to Definitions > Custom URL category.
2. In the Categories area, click + to add a new custom URL category.



3. Enter a name for the Custom URL category.
4. Enter the domain or list of domains separated by a comma.
5. Click **Save**.

Deleting Definitions

1. Navigate to **Definitions**.
2. Click on the definition type that you want to delete whether Network/Service/File/Time Category. The corresponding definitions list is displayed.
3. Select the definitions that you want to delete and click the **Delete** icon.

   Note: Definitions that are in use cannot be deleted but can be edited.

Chapter

6

Policies

You can create various policies that can be applied to users and groups. These policies help you enforce restrictions on the network usage, schedule access time for Internet, identify URLs that must be restricted, create file blocking policies for mail attachments or use the keyword blocking that helps block content containing specific content by keywords.

Note: To apply any policy you need to go to User management > Users and Groups and

apply policies there.

URL Categorization

You may want to block some Web sites on your network for some of the following reasons:

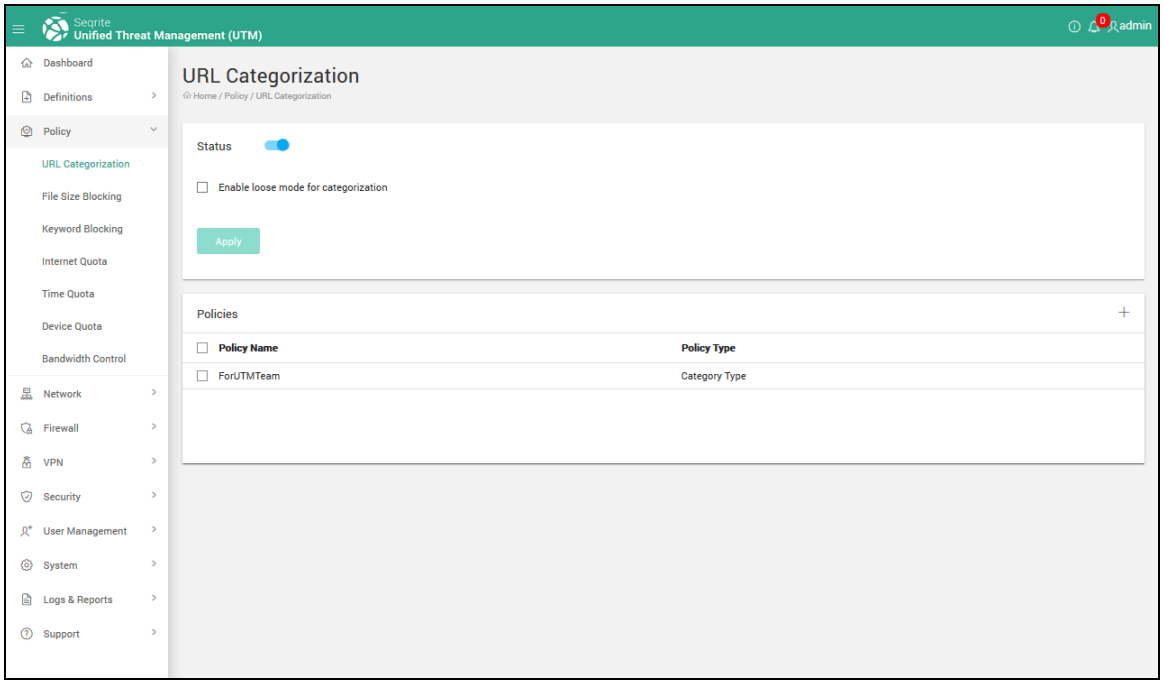
- Inappropriate content, which may be offensive and illegal in nature.
- Entertainment Web sites with streaming content leading to wastage of company's bandwidth.
- Social Networking sites that are not productive for your employees.
- Untrusted Web sites that have malware, Trojans, or viruses.
- Restricting available Web sites to increase the organizational work efficiency.

In URL categorization by Category Type, Seqrite UTM lets you create policies using which you can filter content based on categories or based on blacklisted and Whitelisted domains. You can decide the action to be taken when user accesses websites under these categories based on the content. For e.g. Automobile, Jobs, Downloads, can be moved under denied categories. However when you do URL categorization by domain, you can only select domains to be White listed for the applicable **Time category.**

Note: If Seqrite UTM is in offline mode and Web Security service is set to be offline then the URL categorization will not work.

Enabling URL categorization

1. Navigate to **Policy > URL categorization**.



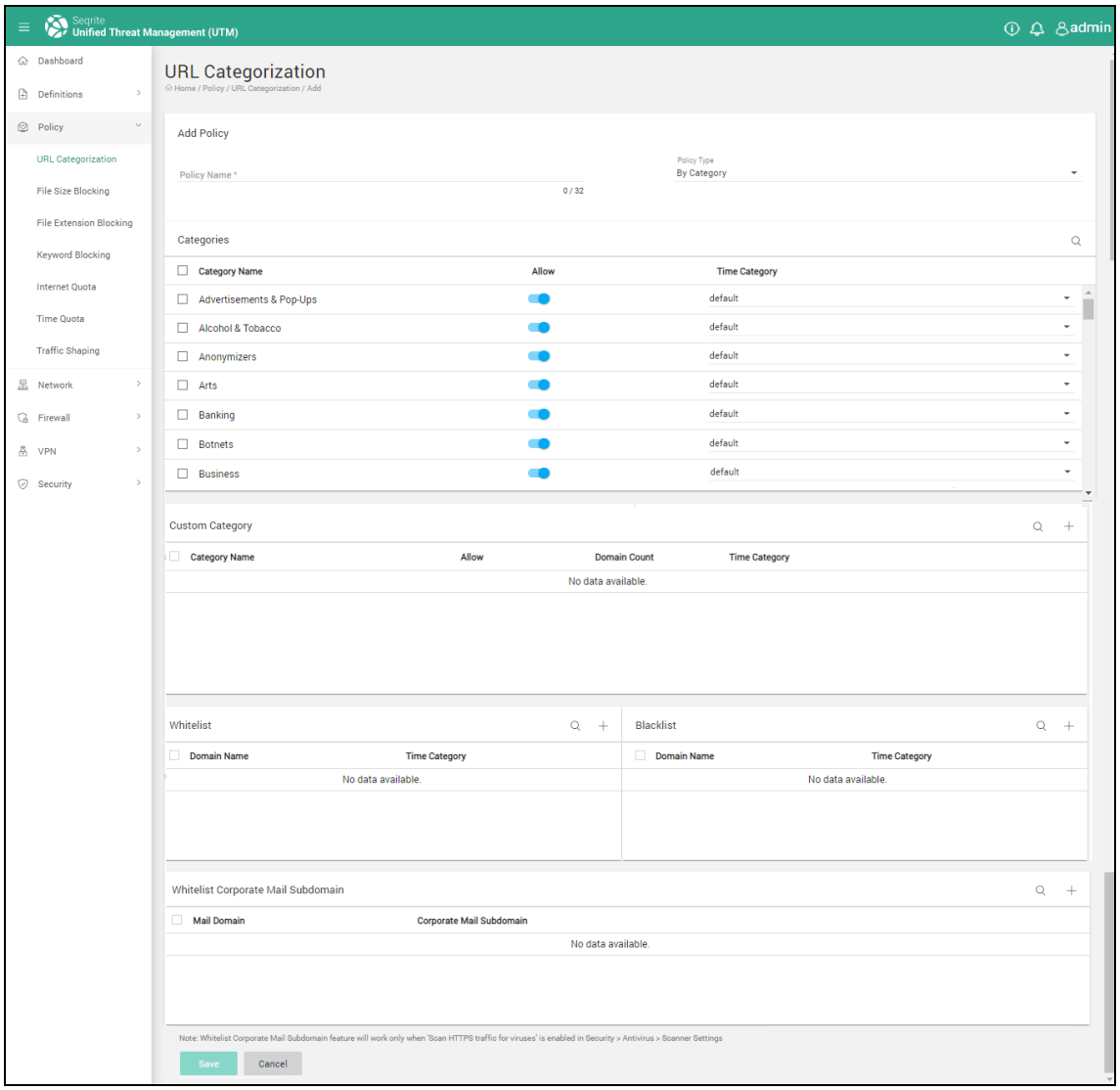
2. Click the status button to enable URL categorization. URL categorization is turned off by default.
3. Enable loose mode for categorization, to improve performance if your network latency is high.
4. Click **Apply**.

URL categorization (By Category type)

You can do URL categorization by Category Type. When you select by Category Type, you can select categories to be blocked and apply the defined **Time category**. You can allow domains under a blocked category by adding these domains to the Whitelist.

Adding a URL category policy

1. Navigate to **Policy > URL Categorization**. The URL Categorization policy page displays the list of policies created.
2. In the Policies section, click the **+ (Add)** to add a new policy based on URL categorization. The following page is displayed.



3. Enter the policy name. Select the policy type as **By Category**.
4. From the list of categories displayed, select the category or categories, the corresponding action whether to block or allow, and the applicable **Time category**.
5. Click **Save**. The policy will be saved and added in the list of URL Categorization policies.

Making Exceptions for URL categorization

If you have blocked a particular category, but still want to allow a domain that falls under that category, you can add that domain to the Whitelist for that policy. Similarly, if you want to block a particular domain that falls under a category that you have allowed access, you can add that domain to the blacklist so that it is blocked. Domains/IP addresses added to a Blacklist are blocked and domains/IP addresses added to a Whitelist are trusted and allowed regardless of whether that category is allowed or blocked.

Adding domain/IP addresses to Whitelist

Use this procedure to allow some

1. Navigate to **Policy > URL Categorization**.
2. In the WhiteList section, click **+ (Add)** to add a new policy**.**
3. Add a domain or an IP address.
4. Select the **Time category** to which the policy would be applied.
5. Click **Save**. The domain is added in the White List and the policy is displayed in the list.

Adding domain/IP addresses to Blacklist

1. Navigate to **Policy > URL Categorization**.
2. In the Blacklist section, click **+ (Add).**
3. Add a domain or an IP address.
4. Select the **Time category** for which the policy will be applied.
6. Click **Save.** The domain is added in the Blacklist and the policy is displayed in the list.

Removing domains/IP address from Whitelist

1. Navigate to **Policy > URL Categorization**.
2. In the Whitelist Policies section, select a policy from the displayed list.
3. Click the **Delete** icon. The websites are deleted from the Whitelist.

Removing domains/IP address from the Blacklist

1. Navigate to **Policy > URL Categorization**.
2. In the Blacklist Policies section, select a policy from the list that is displayed.
3. Click the **Delete** icon. The website is removed from the Blacklist.

Modifying URL categorization policy

1. Navigate to **Policy > URL categorization**. The policies are listed.
2. Select the policy that you wish to edit, the edit icon is displayed.
3. Click the **Edit** icon and modify the policy as required. You can change the status of Block/Allow or change the corresponding Time category.
4. Click **Save**. The modified policy is saved.

URL Categorization policy (By Domain Type)

There may be some websites that you can allow the users to access based on their job profile or business requirements. Adding these Web sites to the White List ensures that users in your network can access the sites mentioned in the list. You can either add the domain name, URL or the IP address of the Web sites. You first need to add a policy and then in the corresponding Blacklist and Whitelist, add the domain/IP addresses that you want to block or allow.

Note: When you create and apply a URL categorization policy by domain, only the domains that are whitelisted are accessible. All other domains will be blocked.

Adding a URL categorization policy by domain type

1. Navigate to **Policy > URL Categorization**.
2. In the Policies section, click **+ (Add)** to add a new policy.
3. In the Policy type drop-down, select By Domain. The White List section is displayed.
4. Click **+(Add)** to add a domain/IP address to the White List. You can add a domain or an IP address.
5. Select the **Time category** for which the policy will be applied.
6. Click **Save**. The domain is added in the White List and the policy is displayed in the list.

Removing Domain/IP addresses from the White list

1. Navigate to **Policy > URL Categorization**.
2. In the Policies section, select the required categorization policy (by domain Type) and click the **Edit** icon. The corresponding Whitelist is displayed.
3. Select the domain name that you want to remove and click the **Delete** icon.
4. Click **Save**. The websites are removed from the Whitelist.

Modifying URL categorization policy

1. Navigate to **Policy > URL categorization**. The policies are listed.
2. Select the policy that you wish to edit, the **Edit** icon is displayed.
3. Click the **Edit** icon and modify the policy as required.
4. Click **Save**. The modified policy is saved in the Policies List.

Adding corporate mail domains to Whitelist

You may require to block gmail.com to prevent your users from accessing their personal email. At the same time, however you may need to allow users access to the corporate email accounts on the same provider, gmail.com. You can do this by adding your corporate Sub domain in the Whitelist Corporate Mail Subdomain section.

1. Navigate to **Policy** > **URL Categorization**.
2. Browse down to the Whitelist Corporate Mail Subdomain section.
3. Click + **(Add)**. The Add Subdomain dialog appears.
4. In the Add Sub domain dialog, enter the Corporate mail Sub domain.
5. Click **Save**. The Sub domain is added, and users will be allowed to access the corporate mail accounts on the Gmail page.

Note: Whitelist Corporate Mail Subdomain feature will work only when 'Scan HTTPS traffic for viruses' is enabled in **Security > Antivirus > Scanner Settings**.

Creating a policy using Custom category definitions

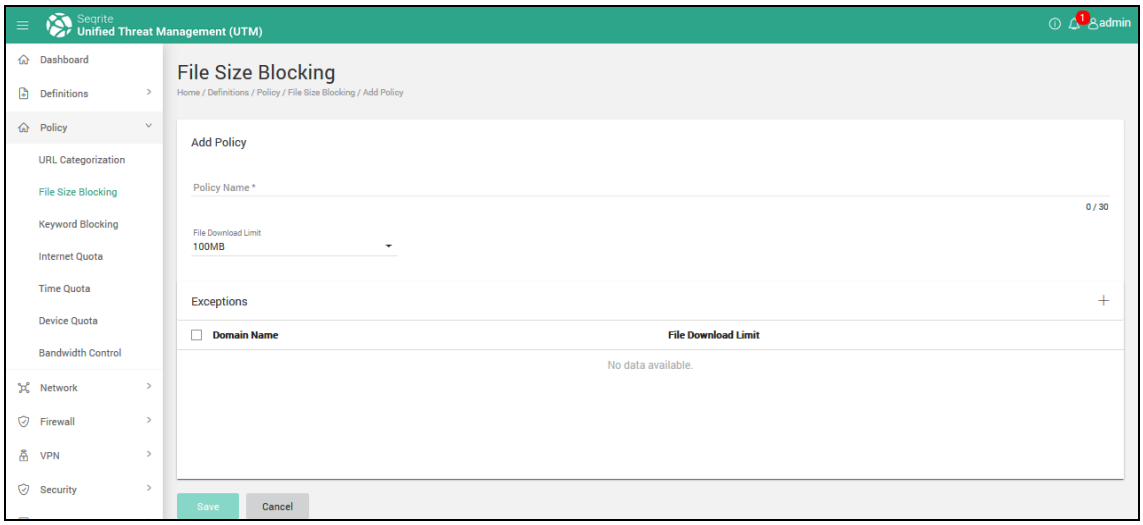
1. Navigate to **Policy > URL categorization**.
2. In the Policies area, click + to add a new policy for above created Custom Category.
3. Under the Add Policy area, enter a name for the policy.
4. Select the Policy type as By Category.
5. Browse down to the Custom Category section.
6. Click + to add a new policy. The definitions dialog appears.
7. From the existing definitions, select the Custom Category created earlier. To create a new Custom Category definition, click the Create Definition button, enter the required information and click **Save**.
8. Click OK. The selected category appears under the Custom URL category area.
9. Toggle the Allow button to enable the Allow/Deny permission for this category.
10. Select the Time category if applicable.
11. Click **Save**. The policy is listed in the Policies area under URL categorization.

Blocking based on file size

You can create a policy to block file attachments from download or upload based on the size. You can also make some exceptions to the rules if required.

Policies

1. Navigate to **Policy > File size Blocking**. The existing policies are displayed.



2. Click the **+ (Add)** icon to add a policy.
3. Enter a name for the policy.
4. Select the file download limit from the drop-down, if required use the custom option to enter a custom size.
5. In the Exceptions area, click the **+ (Add)** icon to add any exceptions to above policy. You need to specify the domain name and file size which will be excluded from the blocking policy.
6. Click **Save** to save the exception. The exception is saved and displayed in the list.
7. Click **Save** to save the policy.

File extension-based blocking

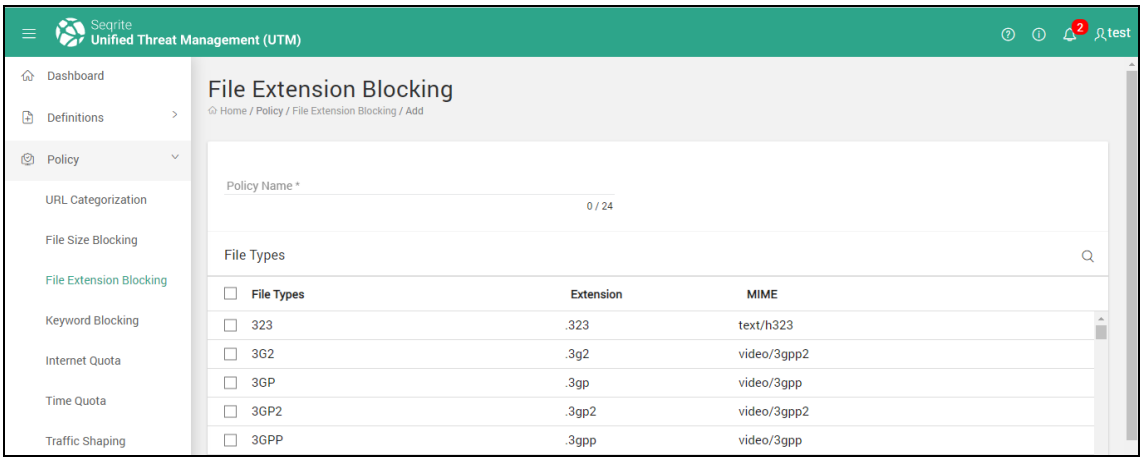
You can create a policy to block files of a certain type based on the extension of the file. For e.g. docs, jpg or .xls files. After the policy is created, you can apply the policy to users or groups.

Note: File extension blocking is based on extension only and not by MIME types.

Creating a File extension-based blocking policy

1. Navigate to Policy > File Extension Blocking.
2. Click the + (Add) icon on the righthand side to create a new File extension blocking policy.

Policies

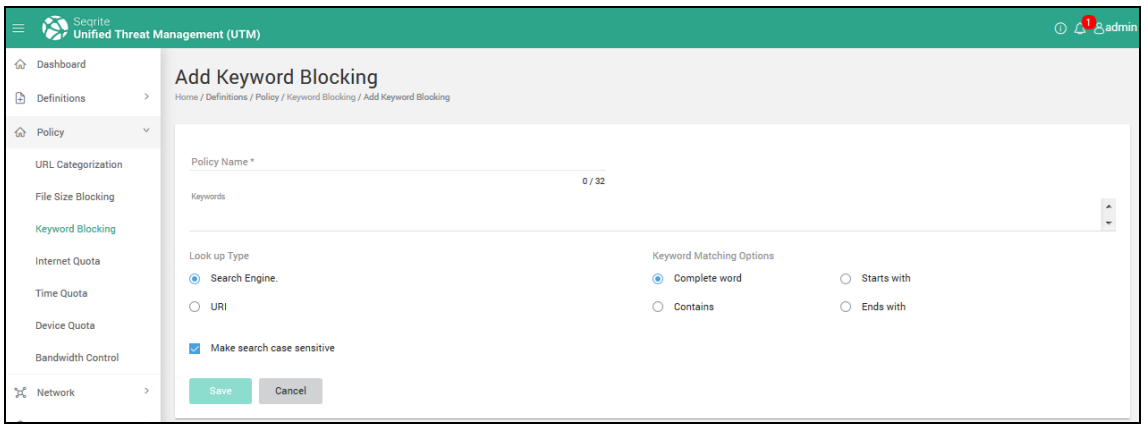


3. Enter a policy name.
4. Select the file type from the displayed list.
5. Click **Save**. The policy is saved.

Blocking based on keywords

You can create a policy to block content based on the keywords defined in the policy. Seqrite UTM will then look up the search engine or the URL to check for the keywords that need to be blocked. Key matches can be set based on starting with or containing a particular string. You can also make the keyword search case-sensitive.

1. Navigate to **Policy > Keyword Blocking.** The existing policy list is displayed.
2. Click **+(Add)** to add a new policy.



3. Enter a name for the policy.
4. In the Keywords field, enter the keywords separated by a comma.
5. Select the Lookup type, whether search engine or URL.

6. Select the appropriate keyword matching option for the string whether complete word, starting with, contains or ends with a particular string.
7. You can choose to make the search case-sensitive by enabling the designated option.
8. Click **Save**.

Internet Quota

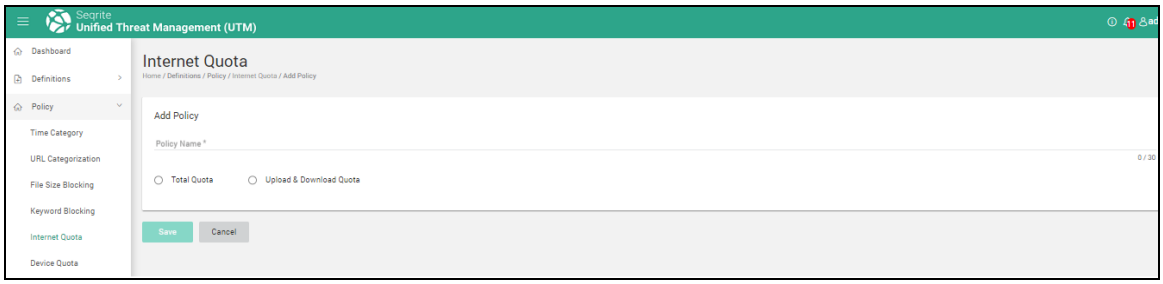
Internet Quota helps to monitor and control the Internet usage for a group and / or a user. You can setup Internet quota policies based on data transfer that can be either Total Data Transfer (upload + download) or individual Upload or Download.

Using the Internet Quota page you can create predefined Internet Quota policy. These policies will be applied to Groups / users. If the group / user reaches the assigned quota, the Internet access will be blocked.

Configuring Internet quota policy based on Total Quota

1. Navigate to **Policy > Internet Quota**. The Internet Quota page is displayed with list of Internet Quota policies if already configured.
2. Select status as **Enabled**.

   Note: Enabling Internet Quota may affect your network throughput. Bandwidth usage reports are not generated if you disable Internet Quota.
3. In the Policies section, click the **+ (Add)** icon, the Add Internet Quota page is displayed.



4. Select the option for Total Quota.

The following table describes the options that are displayed, configure as required:

Field	Description
Policy Name	Enter the Policy name.
Quota frequency	Allows you to set the time period for quota renewal cycle. The following options are available: Once, Daily, Weekly, Monthly, and Yearly. Configure as required.

Field	Description
Unlimited	If you select Unlimited option, there would be no limit on the maximum data usage.
Limited	If you select Limited, then you need to specify the maximum limit in MB.

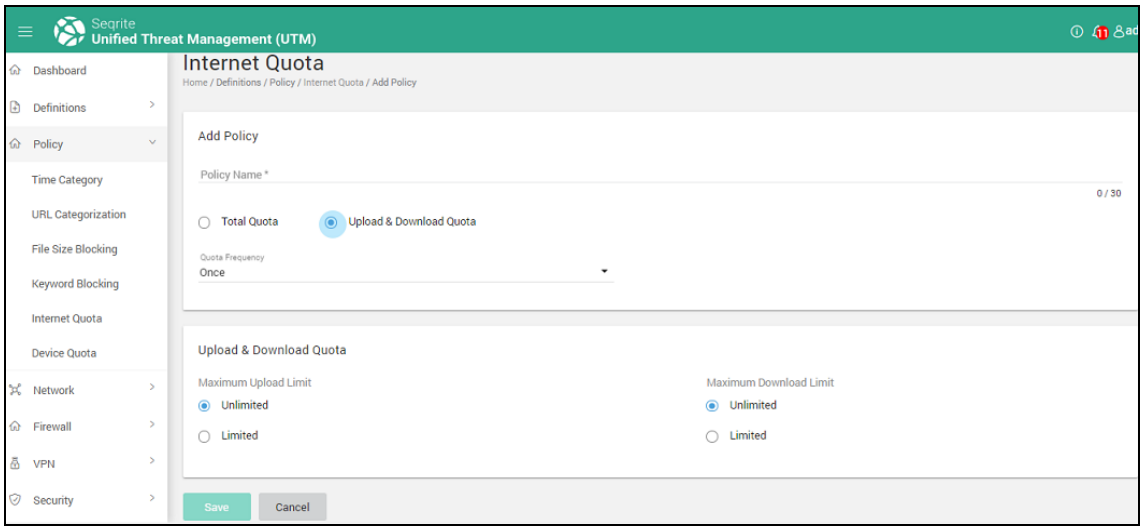
Note: If there is unused data for a period, then that remaining data usage will not lapse. For e.g. If a daily data usage of 100 MB is set for a user and the maximum limit is 1000 MB. Now if the user has consumed 70 MB of data from the daily 100 MB limit, then total remaining data usage will be 930 MB and not 900 MB. According to the Daily usage policy, next day the user will again have 100 MB of data usage for that day and so on. Same is applicable for other frequencies, except for “Once”.

5. Click **Save**. The policy is saved and added to the list.

Creating an Internet Quota policy based on Upload and Download usage

1. Navigate to **Policy > Internet Quota**. The Internet Quota page is displayed with list of Internet Quota policies if already configured.
2. Select status as **Enabled**.

   Note: Enabling Internet Quota may affect your network throughput. Bandwidth usage reports are not generated if you disable Internet Quota.
3. In the Policies section, click the **+(Add)** icon, the Add Internet Quota page is displayed.



4. Select Upload and Download Quota.

   The following options are displayed, configure as required:

Field	Description
Policy Name	Enter the Policy name.
Quota frequency	Allows you to set the time period for quota renewal cycle. The Internet access limit will be allowed from a maximum data limit. The following options are available: Once, Daily, Weekly, Monthly, and Yearly. If you select Quota Frequency as **Once,** select the Maximum Upload and Download limits from options Unlimited and Limited. If you select Limited, you must specify the limit in MB/User for each category. If you select Quota Frequency as **Weekly**, select the starting day under Week starts from drop-down, specify the weekly upload and download limits in MB/User. If you select Quota Frequency as **Monthly**, select the starting date, and month under corresponding drop-down options and specify the Monthly upload and download limits in MB/User. If you select Quota Frequency as **Yearly**, select the starting month under Month starts from drop-down, specify the Yearly upload and download limits in MB/User. **Note**: If there is unused data for a period, then that remaining data usage will not lapse. For e.g. If a daily data usage of 100 MB is set for a user and the maximum limit is 1000 MB. If the user has consumed 70 MB of data from the daily 100 MB limit, then total remaining data usage will be 930 MB and not 900 MB. As per the Daily usage policy, next day the user will again have 100 MB of data usage for that day and so on. This is applicable for all other frequencies, except for "Once".

5. Select the Maximum Upload limit and Maximum Download limit as required.
   Note: Selecting the **Unlimited** option removes any limit on the maximum upload or download data usage. Enter the corresponding limits as required if you select Limited option for both Maximum Upload and Maximum Download data.
6. Click **Save**. The policy is saved and listed.

Editing Internet Quota policy

1. Navigate to **Policy > Internet Quota.** The policies are listed.
2. Hover above the policy you want to edit. The Edit icon is displayed against the policy.
3. Click the corresponding Edit icon and modify the policy as required.

4. Click **Save**.
5. You will be asked to confirm that Quota will be reset. Confirm and proceed with the changes.

   Note: The edited policy is not applied unless you select and click **Apply**.

Deleting an Internet Quota policy

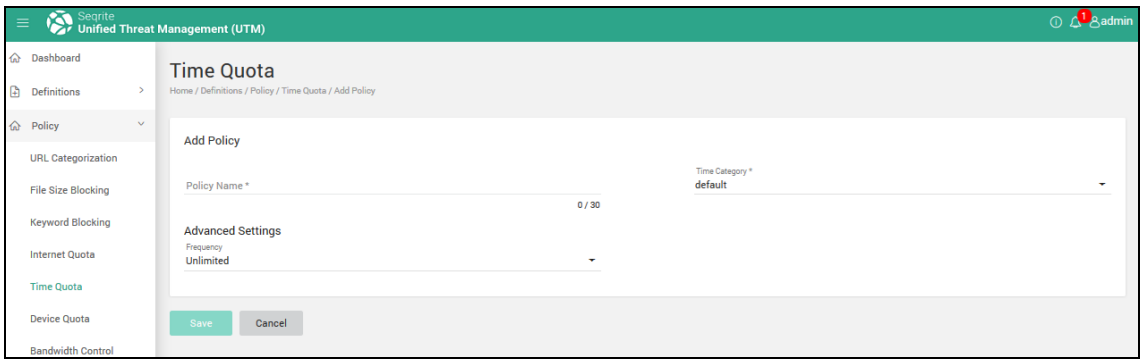
1. Navigate to **Policy > Internet Quota.** The policies are displayed.
2. Hover above the policy you want to delete, the Delete icon is displayed.
3. Click the **Delete** icon. To delete multiple policies, first select and then click the **Delete** icon on the upper right corner.
4. Click **Yes** on the Delete confirmation dialog box that is displayed. The policy is deleted.

Time Quota Policy

The Time Quota policy on Seqrite UTM helps to provide a pre-defined Internet surfing time to users and groups. All available time policies are displayed along with their details, such as, name, access time and description.

Creating a time quota policy

1. Navigate to **Policy > Time Quota.** The time quota policy list is displayed.



2. Click the **+** (**Add)** icon on the upper right corner. The Add Time Quota policy page is displayed.
3. Enter a policy name and select the applicable Time category from the drop-down.
4. In the Advanced Settings area, select the frequency whether daily, weekly, monthly or yearly, and configure the corresponding fields as required. You can create and deploy time-based quota policies based on frequency and data usage limits. For e.g., daily, weekly, monthly, or yearly and data usage.
5. Click **Save**.

Traffic Shaping

You can use the traffic shaping options available in Seqrite UTM to control the flow of network traffic. Network traffic shaping ensures that the desired traffic gets through. Using Traffic Shaping you can create policies that restrict 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.

For users, you can create two types of policies, Shared and Individual. You can create user groups according to requirements and apply the policies as required.

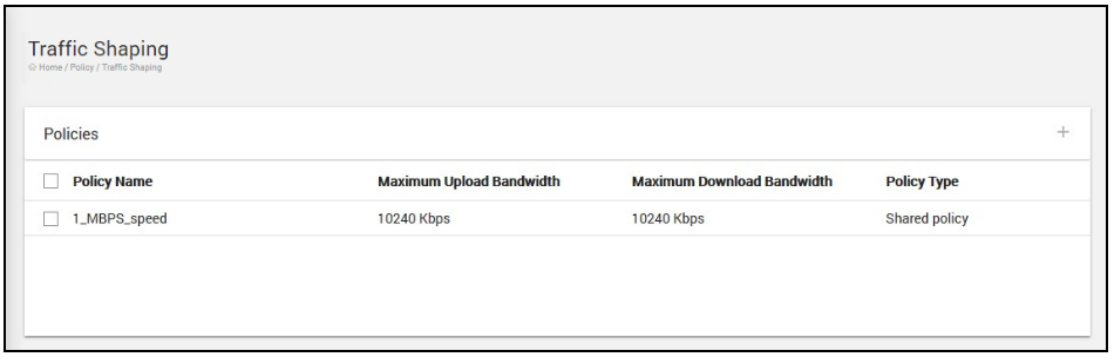
- **Individual**- In this policy, all users in the group to whom this policy is applied will receive the specified bandwidth. For e.g. if you have specified an Upload bandwidth of 10 Mbps and a download bandwidth of 100 Mbps, and apply the policy to a group, each member of that group will get a dedicated bandwidth of 10 Mbps for Upload and 100 Mbps for download.
- **Shared**- In this policy, all the members of the group to which this policy is applied will share the specified bandwidth equally. For e.g. if you have specified an Upload Bandwidth of 100 Mbps and a Download Bandwidth of 1000 Mbps, and if there are 5 active users in the group to which this policy is applied, then each user of the group will get an effective bandwidth of 20 Mbps for upload and a 200 Mbps bandwidth for download. The specified bandwidth will be shared equally among the live users.

Example 1: Users that belong to top management may require a dedicated bandwidth as their usage is high and critical. All such users can be put in a group and an Individual policy with required Upload and Download bandwidth can be applied to that group.

Example 2: Normal users, a group can be created and a shared bandwidth policy when applied ensures that the specified bandwidth is shared across all users of that group.

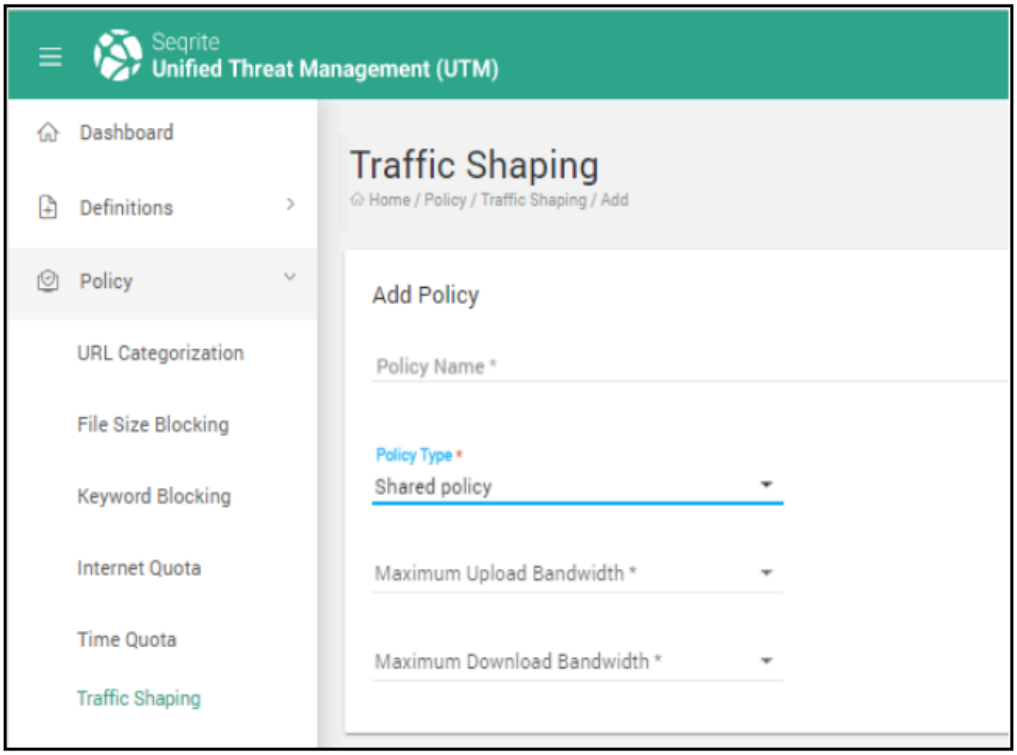
Creating a Traffic Shaping policy

1. Navigate to **Policy > Traffic Shaping**. Existing policies if any are displayed.

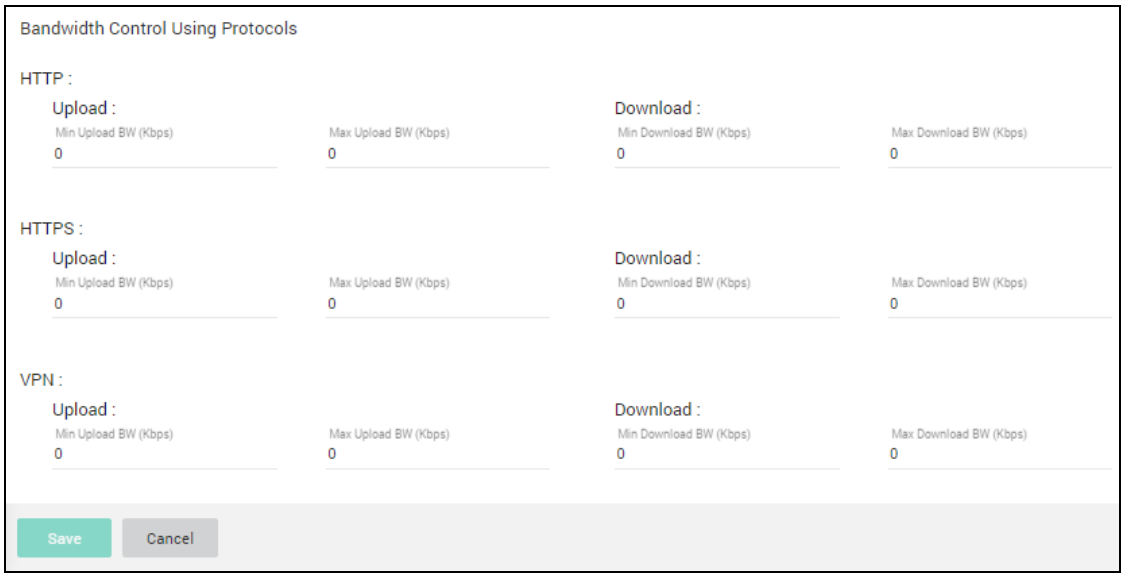


2. Click the **+ (Add)** icon to add a new policy.

Policies



3. Enter the name for the policy.
4. Select the type whether Shared or Individual.
5. Select the Maximum Upload and Download bandwidth as per the requirement. If you select Custom, specify the required bandwidth.



Note: The Maximum Upload and Download limits specified under VPN are applicable only to the remote hosts of IPsec Site-to Site and SSL Site-to-Site VPN link.

6. Click **Save**. The policy is saved. This policy can be then applied to users in the User Management section as required.

Chapter 7

Network Configuration

Interfaces

Interfaces are the physical and virtual ports on the Seqrite UTM. The number of interfaces depends on the Seqrite UTM model. Using the interface page, you can add, edit, and delete Interfaces, Aliases, VLAN, and Bridge. You can also set an interface as default.

Seqrite UTM supports three zones namely LAN, WAN and DMZ. Each interface must be configured for one of these zones.

Zone

- **LAN:** This is your company's internal network. In Seqrite UTM, interfaces that are configured for internal network can be assigned to be part of LAN zone.
- **WAN:** This is the external network that is the Internet. In Seqrite UTM, interfaces configured for external network can be assigned to be part of WAN zone.
- **DMZ:** Demilitarized zone (DMZ), is a small sub-network that is located between a trusted internal network, such as your company's private LAN, and an untrusted external network, such as the Internet. Internal network which has servers such as webserver, mail server etc. that are to be accessed from untrusted network(s) or Internet can be kept in DMZ zone.

By default, LAN to WAN zone traffic such as HTTP, HTTPS, SMTP, POP3 and SSH is allowed. All inter-zone traffic is blocked.

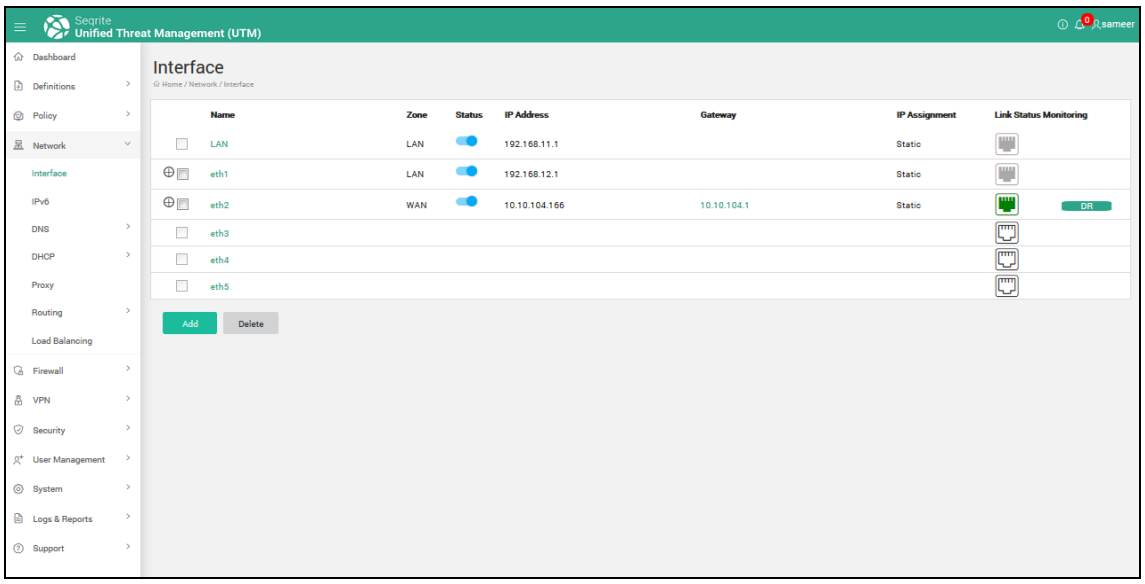
Configuring Interfaces

The Interface page displays the list of all the default interfaces. These interfaces are the ports on the Seqrite UTM appliance. The Alias and VLAN interface that are added under the default ports are displayed in the interface list as a sub-interface of the base interface.

The following table explains the color used to indicate the interfaces.

Icon	Description
	Indicated that Ethernet cable is connected.
	Indicates that Ethernet cable is connected, and Internet is available.
	Indicates that Ethernet cable is connected & and Internet is not available.
	Indicates that Ethernet cable is not connected.
	Indicates that a WIFI connection is available Applicable only for the NGS130W model.

1. Navigate to **Network > Interfaces**. The Interfaces list is displayed.



2. Click **Add** to add an interface. To modify an interface, click the interface name in the list. The corresponding settings for the interface are displayed. Configure the settings as required:

   The following table explains the fields on the page. Note: The fields are displayed based on the corresponding settings, some fields may not be available as per the settings.

Field	Description
Type	Select the type from the drop-down whether Alias, VLAN, Bridge, Link

Field	Description
	Aggregation.
Interface name	Enter a name for the interface.
Zone	Select from LAN, WAN, and DMZ.
Base Interface	Select whether eth0, eth1, or eth2
IP assignment	This can be Static, PPPoE, or DHCP. Note: PPPoE and DHCP options are available only if WAN zone is selected. If you select the IP assignment as **Static,** then you need to enter the IPV4 address and Subnet mask. If you select the IP assignment as **PPPoE** then you need to enter the user name and password provided by your ISP. Note: To view Live Logs for **PPPoE** service, Go to Logs and Reports > Live Logs. Select the required module(s) and click Export. The logs are exported in a .txt document to your computer. These logs indicate the current status of the selected module.
IPv4 Address	This field is displayed if you select IP assignment as Static. Set IPv4 address for the Seqrite UTM, through which all clients will access the Internet.
Subnet mask	This field is displayed if you select IP assignment as Static. Select the appropriate Subnet mask.
IPv4 Gateway	This field is displayed if you select IP assignment as Static. Set the gateway if Seqrite UTM is behind the router. Note: If gateway is set for WAN interface then for LAN interface gateway cannot be set.
IPv6 Address	This field is displayed if IPv6 is enabled. For more details see **IPv6**. Enter the IPv6 address through which all clients will access the Internet.
Prefix	This field is displayed if IPv6 is enabled. For more details see **IPv6**. Enter the prefix.
IPv6 Gateway	This field is displayed if IPv6 is enabled. For more details see **IPv6**. Enter the IPv6 Gateway.

Field	Description
User Name	This field is displayed if you select IP assignment as Dialup. Enter the username provided by ISP.
Password	This field is displayed if you select IP assignment as Dialup Enter the password provided by ISP.
Service Name	This field is displayed if you select IP assignment as Dialup. Enter the Service name provided by ISP.
Hardware address	Displays the actual MAC id for that interface.

3. Click **Apply** to save the changes if any.

Editing an interface

1. Navigate to Network >Interfaces. The Interfaces list is displayed.
2. Click on the Interface that you want to edit. The edit interface screen is displayed.
3. Correct the Interface name, Zone, IP assignment, IPV4 address, subnet mask and gateway IP address as required. Use the Redial IP button to connect to the dialup server if you have selected the IP assignment as PPPoE. The IP address is assigned automatically. If you have selected DHCP option, click the Renew IP option to assign the IP.
4. Select the Link change method and Detection IP as required. The link check methods check if the interface is up and connected. You can configure the method as ICMP or DNS. Seqrite UTM pings the configured DNS or IP to check if the interface is up and connected.
5. If you want this interface to be default route, place a check mark against the option.
6. Click **Apply**.

Deleting Interfaces

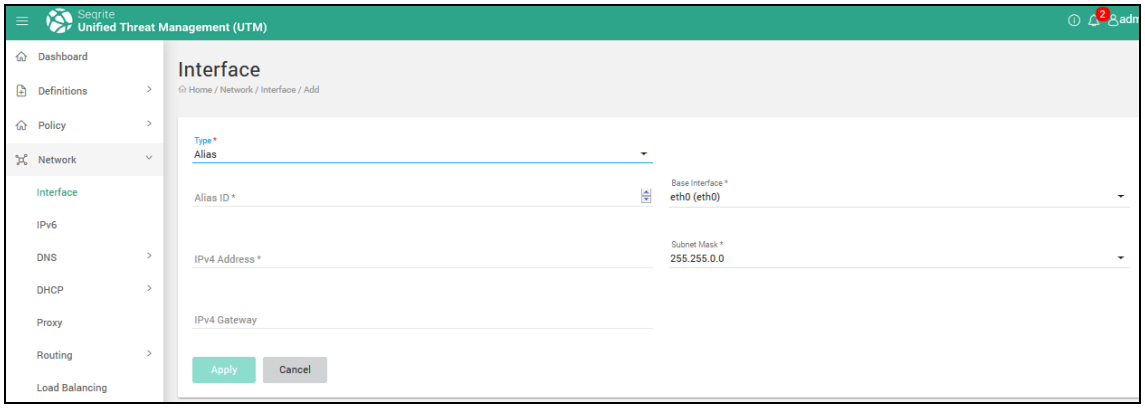
1. Navigate to **Network > Interface**. The Interfaces list is displayed.
2. Select the Interface that you want to delete and click the **Delete** icon. A confirmation message is displayed.
3. Click **OK** to confirm deletion of the interface.

   Note: You cannot delete interface eth0. Deleting the interfaces will only clear the configuration / settings, the port will still be displayed in the list.

Adding Alias

Adding an Alias interface allows you to configure multiple IP addresses to a single physical interface / port. Adding Alias feature gives the base interface another identity and can be used to connect to different logical network subnets. The zone of base interface is the zone of Alias.

1. Navigate to **Network > Interface**. The Interface details page is displayed.
2. Click **Add**. The following page is displayed.



3. Select the type of Interface as **Alias**.

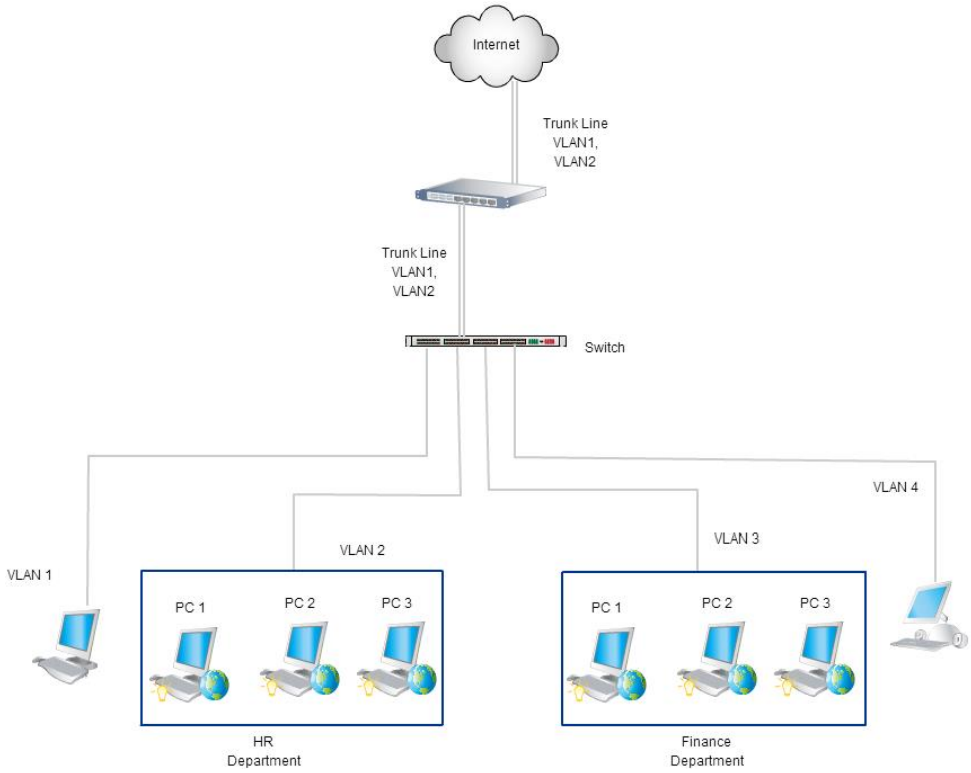
   Enter the following details:

   - **Alias Id**: This is a unique number used to identify the Alias.
   - Select the **Base Interface**. You can use only the configured interfaces.
   - Enter the **IPv4** IP address.
   - Select the **Subnet mask** as applicable.
   - Enter the **IPV4 gateway** address.
4. Click **Apply**.

   Note: The Alias interface is displayed in interface list as a sub interface of base interface.

VLAN

A Virtual Local Area Network (VLAN) is a group of workstations, servers and network devices with same set of requirements that appear to be on the same LAN despite their geographical location. A VLAN allows a network of computers to communicate in an environment as if they exist in a single LAN. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to change in network requirements and relocation of workstations and server nodes.



Adding VLAN in Seqrite UTM helps to increase the network segments. The VLAN feature allows you to configure multiple VLAN interfaces on a single interface. Seqrite UTM supports the 802.1q VLAN standard.

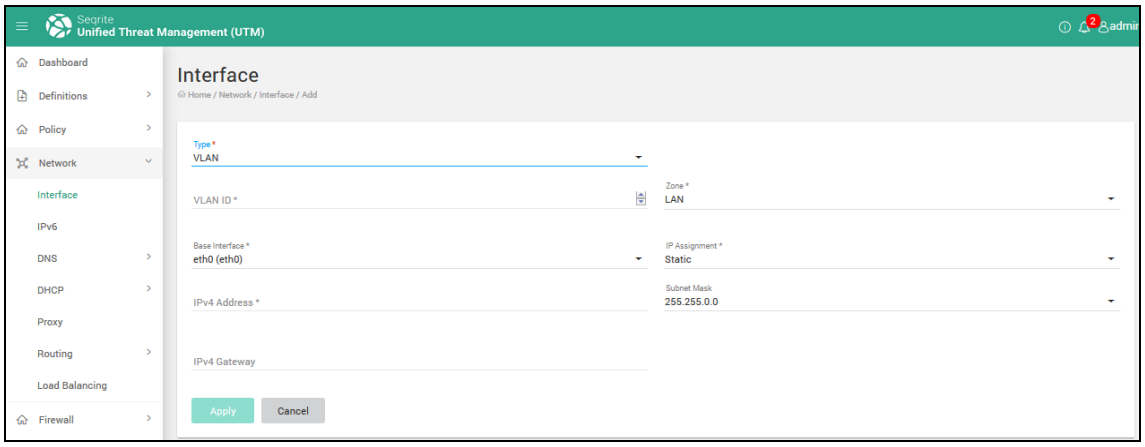
You can create the following types of VLAN:

- VLAN- LAN: For Local Network.
- VLAN –WAN: For external network (Internet)/ ISP.
- VLAN-DMZ: For demilitarized zone, which is a neutral zone between a company's private network and the outside public network.

Note: Adding an interface does not add a physical port on Seqrite UTM. The number of ports will be the same that are the default ports depending on the Seqrite UTM model.

Adding a VLAN

1. Navigate to **Network > Interface**. The Interface details page is displayed.
2. Click **Add**. The following page is displayed.



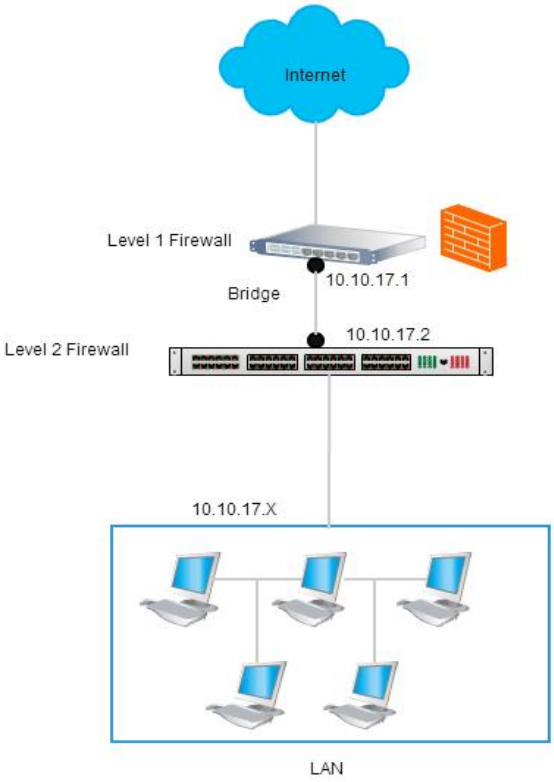
3. Select the type of Interface as **VLAN**. On selecting VLAN, enter the following details:
   - Enter the **VLAN ID**. This should be between the ranges 2- 4094.
   - Select the **Zone** of operation, whether LAN, WAN, or DMZ.
   - Select the **Base Interface** that is the physical port. All the configured and un-configured network interfaces will be displayed here.
4. Select the type of **IP assignment**, whether Static, Dial up, or DHCP.

   Note: For LAN and DMZ interface the IP assignment will be only Static.
   - If you select the IP assignment as Static then you need to enter the IPV4 address, Subnet mask, IPv4 gateway, Link Check method and Detection IP. You can also set the route to be used as the Default route.
   - If you select the IP assignment as PPPoE, then you need to enter the Username and Password provided by your ISP.
5. Click **Apply**.

   Note: Every VLAN interface is displayed in interface list as a sub interface of base interface.

Bridge

Bridge interface is used to connect two network segments within one logical network or to break a collision domain. Seqrite UTM supports IEEE 802.1D standard for configuration of network bridge interface. You can configure Seqrite UTM in bridge mode if you already have a firewall/router and do not wish to replace it. Seqrite UTM supports mixed mode configuration where both bridge mode and router mode can be simultaneously configured on the device. Bridge can be configured only between un-configured interfaces.

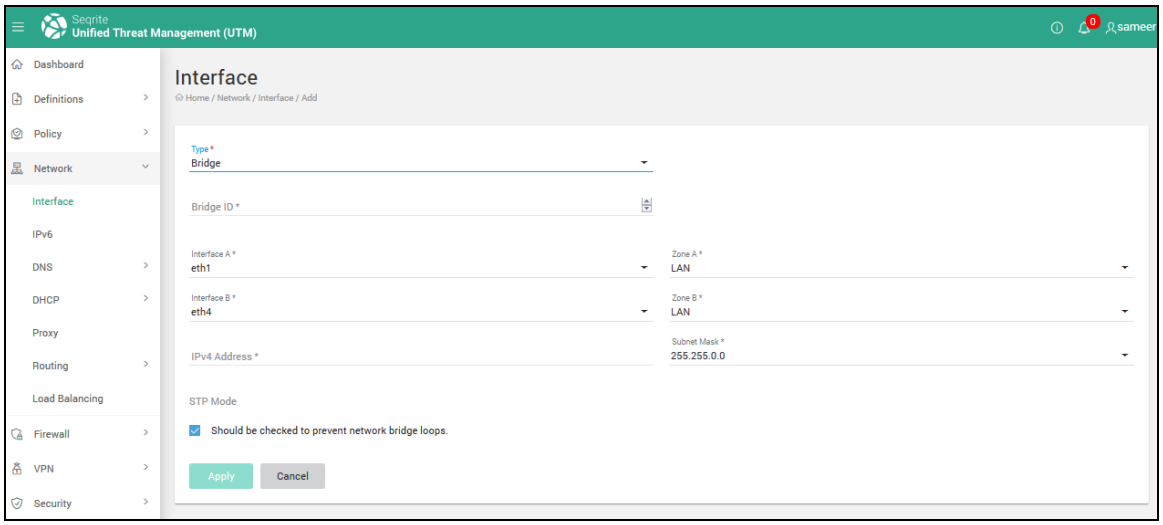


You can use Seqrite UTM bridge interface in the following modes:

- **Transparent gateway:** Seqrite UTM device acts transparently with upstream router/firewall/UTM for the traffic that is passing through the network bridge. You can configure it as a LAN-WAN bridge where network interface, terminated in router will be in WAN zone and interface terminated in switch for local network will be in LAN zone.
- **Local network segment bridge**: In this case, Seqrite UTM device connects to internal network segments i.e. LAN-LAN, LAN-DMZ or DMZ-DMZ bridge.

Adding a bridge interface

1. Navigate to **Network > Interface**. The Interface details page is displayed.
2. Click **Add**. The following page is displayed.



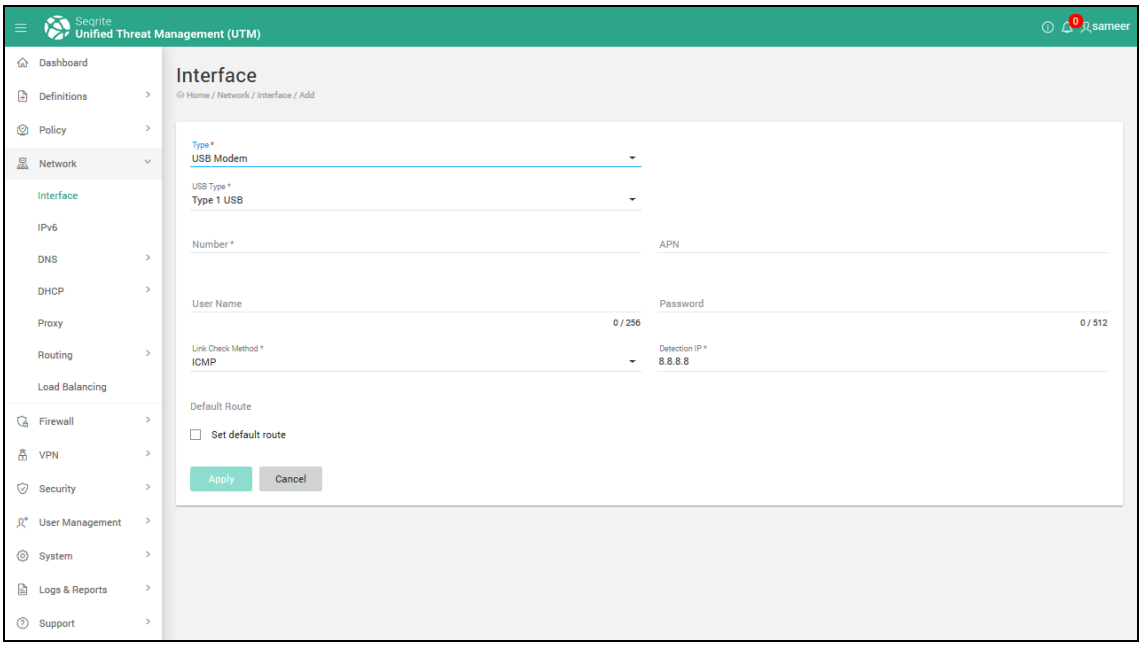
3. Select the **Type** of Interface as Bridge.
4. Adding a bridge requires 2 Seqrite UTM ports. On selecting Bridge, configure the following:
    - **Bridge ID**: This should be between 0- 100. It is a unique number to identify the bridge.
    - Select Interface A and its respective Zone.
    - Select the Interface B and its respective Zone.
    - Enter the **IPv4** address and the corresponding **Subnet mask**.
5. Enter the **IPV4 Gateway** if Seqrite UTM is behind the router.
6. Enable the **STP mode** if required. This option is displayed only for Bridge option. Enabling this mode helps to prevent network bridge loops.
7. Click **Apply**.

USB Modem

Wireless Universal Serial Bus (USB) modems allow computers to wirelessly connect to the Internet via a cellular data network. You can use this feature to access Internet if your WAN links are down. You need to plug in the USB and scan the modem. You can also reset the USB configurations.

Configuring the USB Modem

1. Navigate to **Network > Interface >** Click **Add.** The following screen is displayed.



2. From the Type drop-down**,** select USB modem.
3. In USB type, select **Type 1 USB.**
4. Enter the Phone Number, APN, Username and Password, select Link Check method, and Detection IP address. You can enable the default route to be followed.

Field	**Description**
Phone No.	This is the number dialed by the USB modem to connect to the ISP. Following are the Phone numbers for some networks: GSM/W-CDMA -*99# CDMA - #777 LTE - *99#
Username	Enter the username provided by the ISP for the USB modem.
Password	Enter the password provided by the ISP for the USB modem.

5. Click **Apply**, the USB modem will be connected with the ISP and the details for the detected modem are displayed in the list of the Network Interfaces.

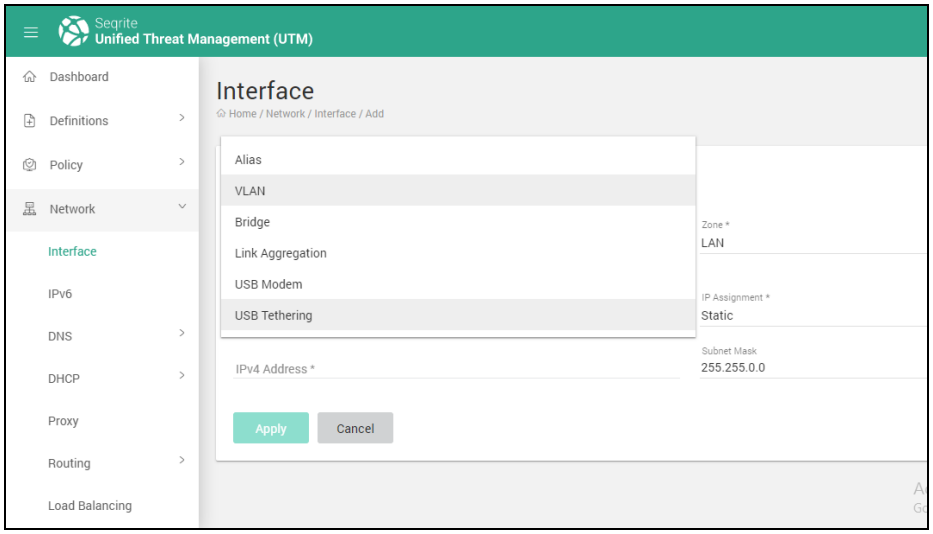
Note: If the USB modem is not recognized, you might need to install a driver. Check for the driver updates from the vendor. You may need to call the Support service for first-time activation of any USB Modem.

If WAN links are down and USB modem is connected, then the USB Modem will be automatically set as Default Route.

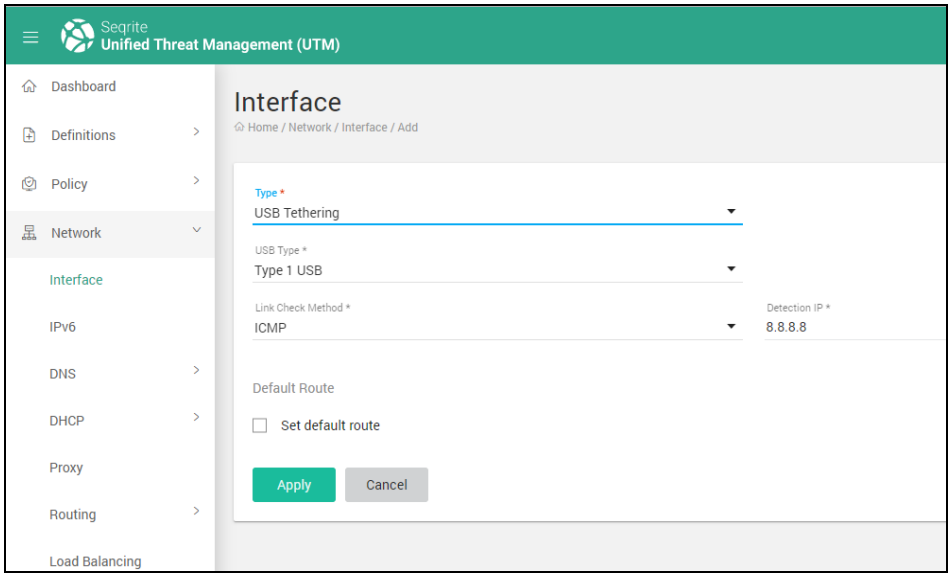
Adding a USB tethering device for Internet connection

You can also use USB based Internet dongles from service providers with UTM.

1. Connect your USB Internet Dongle to the USB port.
2. Navigate to **Network > Interfaces**.
3. Click **ADD**.



4. In the Type drop-down, select USB tethering. The USB Type will be Type 1 USB by default.



5. Select the Link Check Method and the Detection IP address. This is the IP address that UTM will ping at predefined intervals for the link check method. We recommend you keep it as 8.8.8.8.
6. Enable the option for setting default route if you want this USB based Internet connection to be the default route.
7. Click **Apply**.

   Note: To set the USB tethering interface as failover, go to **Network > Load Balancing** and configure the USB tethering interface as required.

IPv6

Internet Protocol (IP) specifies the addressing scheme for computers to communicate over a network. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. It allows you to address a package and drop it in the system.

There are currently two version of IP: IPv4 and a new version called IPv6. IPv4 (Internet Protocol Version 4) is the fourth revision of the IP used to identify devices on a network through an addressing system. IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^32 addresses (just over 4 billion addresses). With the growth of the Internet it is expected that the number of unused IPv4 addresses will eventually be over because every device that connects to the Internet requires an address.

IPv6 is an evolutionary upgrade to the Internet Protocol. A new Internet addressing system Internet Protocol version 6 (IPv6) is being deployed to fulfill the need for more Internet addresses. IPV6 uses increased length of addresses, from 32 bits in IPv4 to 128 bits in IPv6. This increases the total address space size from 232 (about 4.3 billion) to 2128 (about 340 trillion, trillion, trillion). It also doubles the size of the Packet Header, which adds 20 bytes of additional overhead on every packet.

IPv6 uses "coloned-hex" (e.g. 2001:470:20::2) for external data representation, whereas IPv4 uses "dotted-decimal" (e.g. 123.34.56.78). Both IPv4 and IPv6 addresses are represented internally (in memory, or on the wire) as strings of bits (32 of them for IPv4, 128 of them for IPv6). IPv4 addresses are represented externally with 4 fields of 8 bits each, using up to 3 decimal digits in each field (values 0 to 255). Fields are separated by dots (".").

Seqrite UTM supports IPV6 IP format and allows you to enable it. On enabling IPV6 you can use it while configuring the following settings:

- Interface
- DNS
- DHCP

- Content Filtering (Blacklist / whitelist and Domain)

Seqrite UTM also allows you to automatically tunnel IPv6 addresses over an existing IPv4 network. A 6to4 tunnel allows IPv6 domains to be connected over an IPv4 network to remote IPv6 networks.

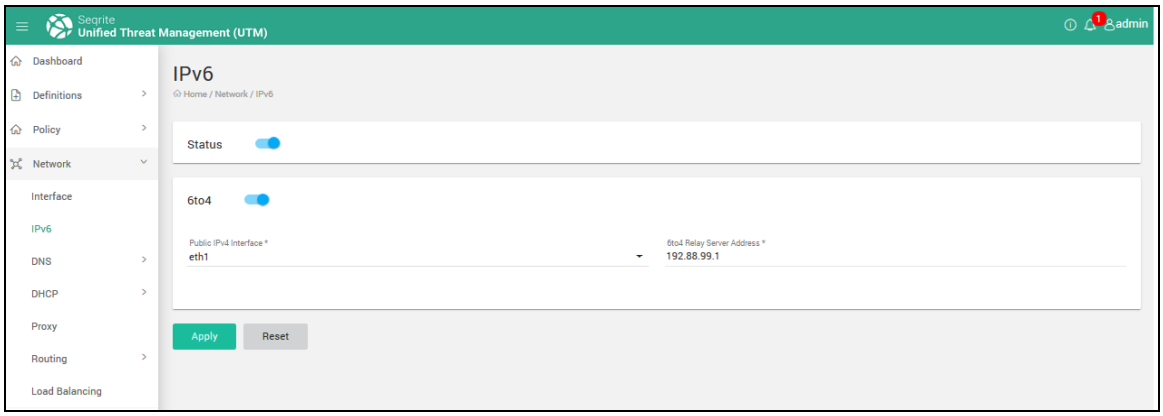
Enabling IPV6

1. Navigate to **Network > IPv6.** By default, IPv6 support is disabled.
2. Toggle the status button to enable **IPV6** and click **Apply**.

Note: You cannot configure any of the settings related to IPv6, unless you enable IPv6 support for Seqrite UTM.

Enabling 6 to 4 tunnel

1. Navigate to **Network > IPv6**. Enable the IPv6 mode.



2. In the **6to4** section, click the status button to enable **6to4.**
3. Select an interface**.** This Interface should be of a public WAN with IPv4 address and on which the 6to4 tunnel is to be created.
   Note: You must configure the WAN interface before enabling the **6to4** tunnel.
4. Select the public IPv4 address.
5. Enter the 6to4Relay Server address. This option helps to set the relay server, you can either enter the address or use the default 192.88.99.1 as relay server.
6. Click **Apply.**

DNS

A Domain name server (DNS) converts domain name into an Internet Protocol (IP) address which is used by computers to identify each other on a network. Domain names are alphabetic and easier to remember by humans. However, the Internet is based on IP addresses. Every time you type a domain name, a DNS service translates the name into the corresponding IP address. With the help of DNS, you do not have to keep your own address book of IP addresses. Instead, you just connect through a domain name server, also called a DNS server which manages a massive database that maps domain names to IP addresses. This process is called DNS name resolution, as the DNS server resolves the domain name to the IP address. For example, when you type the domain name www.example.com in your browser, the DNS server resolves the domain name into an IP address, such as 205.105.232.4.

If a DNS server does not have an IP address of a particular domain name, that DNS server sends a request to another DNS server, and so on, this process continues until the correct IP address is returned.

The DNS feature on the Seqrite UTM allows you to override the default Domain Name Server settings and enter the details of the DNS provided by your ISP or specify a particular DNS that you want to use. You can also change the priority of DNS. This feature allows Seqrite UTM to try to use another DNS server in case the server you are using is unavailable.

Seqrite UTM supports the following types of DNS configurations:

- DNS Servers
- Static DNS
- Dynamic DNS

DNS Servers

Using the DNS Server Settings, you can add the IP address of the DNS provided by your ISP. You can add an IPv4 or IPv6 IP address. An IP address in the IPV4 standard has four numbers separated by three decimals, as in: 70.74.251.42. An IP address in the IPV6 standard has eight hexadecimal numbers (base-16) separated by colons, as shown below:

2001:0cb8:85a3:0000:0000:8a2e:0370:7334.

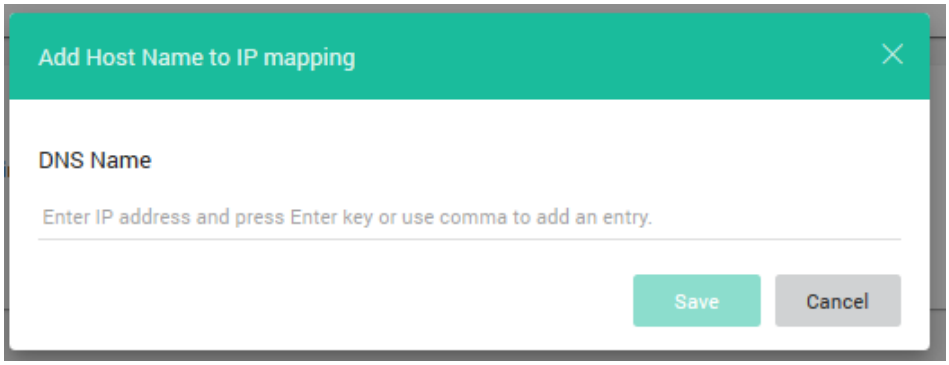
Note: You can add IPv6 DNS only if you have enabled the IPv6 feature on Seqrite UTM. For more details on IPV6 feature see **IPv6**.

By default, the DNS with IP address 8.8.8.8 is used.

Adding a DNS server

1. Navigate to **Network > DNS > DNS Servers**. The DNS page is displayed which contains the list of DNS servers.

2. Click the **+ (Add)** icon displayed on the right-hand corner of the DNS table. The add DNS Servers dialog box is displayed.



3. Enter the IP address of the DNS server and click **Save**.

Deleting Global DNS servers

1. Navigate to **Network > DNS > DNS Servers**. The Global DNS page is displayed which displays the list of DNS servers.
2. Select the server you want to delete and click the **Delete** icon. You can select and delete multiple servers at the same time.
3. Click **Apply**.

Changing the Priority of DNS servers

You can change the order of priority for the listed DNS servers. Changing the priority helps to change the order of searching the DNS server for IP addresses. The top-most DNS server has the highest priority while the DNS server at the bottom has the least priority, i.e. the first DNS server is searched first for the IP address.

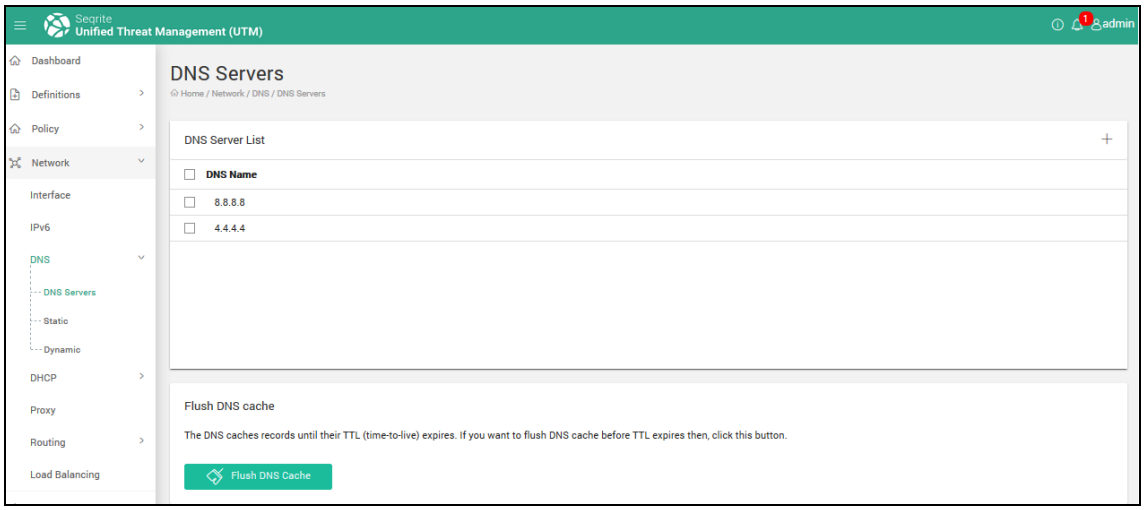
1. Navigate to **Network > DNS > DNS Servers**. The DNS Servers page is displayed with the list of DNS servers.
2. Select the required DNS server whose priority you want to change.
3. Click the arrow buttons that are displayed on the upper right side to move the DNS server names up or down as per the priority.
4. Click **Apply**. The DNS Server list is updated as per the priority.

Flushing DNS Cache

The DNS cache temporarily stores records of all the recent visits and attempted visits to websites and other internet domains. Each of these records has an expiration date (TTL: Time-To-Live) after which the record is deleted. Use the Flush cache option to manually empty the

cache as required if you want recent changes in DNS records to take effect immediately without waiting for the TTL to expire.

1. Navigate to **Network > DNS > DNS Servers**. The DNS Servers page is displayed which displays the list of DNS servers.



2. Click **Flush DNS Cache.** The cache is flushed, and contents are deleted.

Static DNS

If you know the IP address of a host, then you can add a static DNS entry for the hosts in Seqrite UTM. Whenever you access this host, the Seqrite UTM will resolve and return the added IP address.

Adding a Static DNS entry

1. Navigate to **Network > DNS > Static**. The DNS Settings page is displayed with a list of DNS servers. If no DNS servers are listed, you need to add a DNS server.
2. Click **Add icon** to add a new DNS entry. The Add static DNS popup is displayed.

3. Enter the Host Name and IPv4 address, in the designated textboxes.
   Note: The host name must be a FQDN (Fully qualified Domain name).

4. Click **Save**.

Deleting a Static DNS Entry

1. Navigate to **Network > DNS > Static.** The DNS Settings page is displayed which displays the list of static DNS servers.
2. Select the server you want to delete and click the **Delete** icon. You can also select and delete multiple Static DNS hosts at a time.

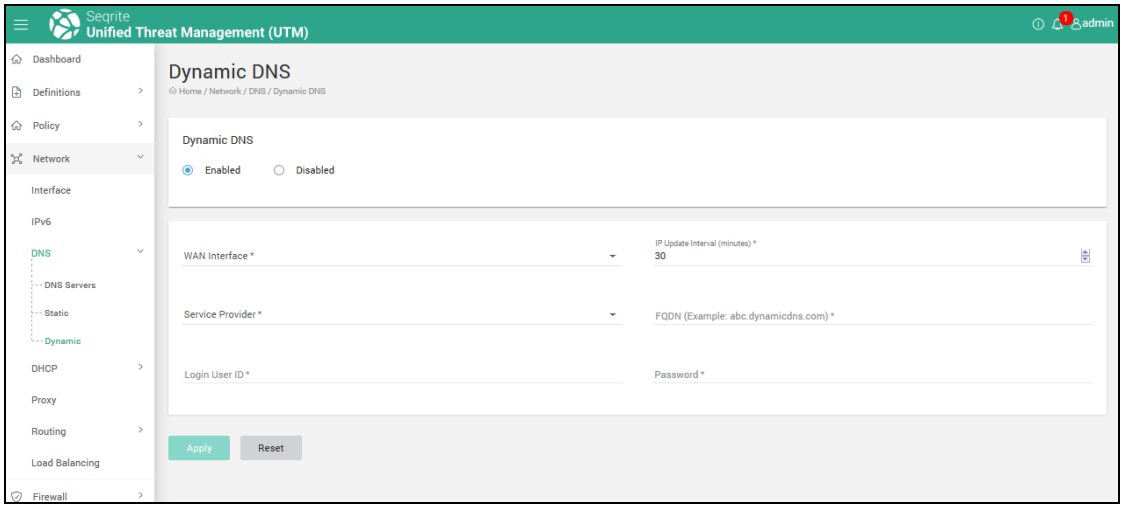
Dynamic DNS

Dynamic Domain Name System (DDNS) helps to link a domain name to changing IP addresses. This service is provided by a DDNS service provider for e.g. Dyndns. The DDNS service provider contacts the DNS service at a specified time interval for the updated IP address and subsequently updates the DNS database to reflect the change in IP address. In this way, even if a domain name's IP address is changed by the ISP, you do not have to remember the changed IP address in order to access the domain.

The Dynamic DNS Feature in Seqrite UTM allows you to configure the DDNS account that you have purchased from the DDNS service provider and bind it to a WAN interface.

Configuring DDNS on Seqrite UTM

1. Navigate to **Network > DNS > Dynamic DNS.** The following screen is displayed.



2. Ensure that the Dynamic DNS is **Enabled**.
3. Select the WAN Interface. This is the WAN interface that you have configured in the Interface section. (See Interfaces for more details.)

4. Select the IP Update Interval (in minutes). Seqrite UTM will sync with the DDNS and check whether there is any change in the IP address and update accordingly after the configured time interval.
5. Select your DDNS service provider.
6. Enter the Host Name that is the fully qualified domain name (FQDN) provided by the Dynamic DNS service provider. For example, abc.dynamicdns.com.
7. Enter the Login User ID and Password of your DDNS account.
8. Click **Apply**.

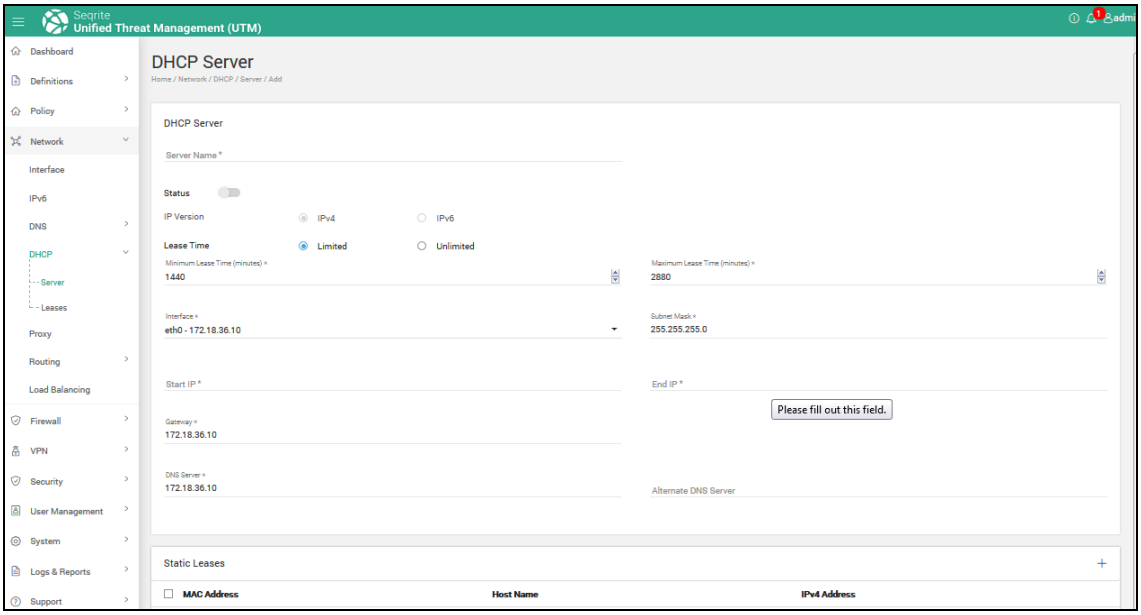
DHCP

Dynamic Host Configuration Protocol (DHCP) allows you to assign IP parameters automatically to your network devices from a DHCP server. The DHCP server feature is useful as it automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway new computers to the network.

Seqrite UTM acts as a DHCP server for your network and assigns IP addresses dynamically in your IT environment. By using a DHCP server, you can also reduce the possibility of an IP address conflict as the IP addresses are assigned dynamically.

Adding a DHCP server

1. Navigate to **Network > DHCP > Server**.
2. Click the **+ (Add)** icon. The Add DHCP server screen is displayed.



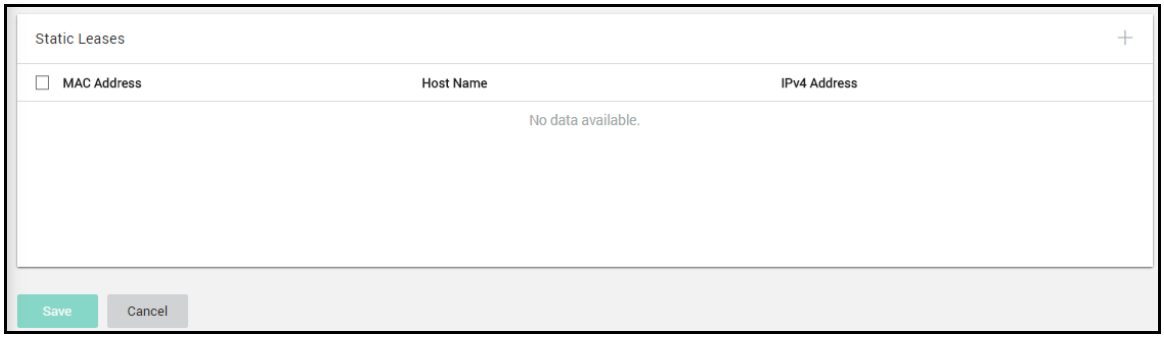
3. Enter a name for the DHCP server.

4. Toggle the DHCP server status button to enable DHCP.
5. Select the type of IP addressing scheme, whether IPv4 or IPv6. If you select IPv4 then DHCPv4 will get configured and IP from given range will be assigned to clients. If you select IPv6 then DHCPv6 will get configured and IP from given range will be assigned to clients.
6. Select the lease time, whether limited or unlimited as required. If you select limited, enter the Minimum and Maximum lease period intervals (in minutes).
   Minimum Lease time is the lease time after which the client will request to renew the lease. Maximum Lease time is the lease time after which DHCP server will free the IP address if no response is returned from the client.
7. Select the Interface from the available interfaces and enter the corresponding subnet mask.
8. Enter the range of the IP addresses in the Start IP and End IP fields.
9. Enter the Gateway IP address. By default, it is the IP address of eth0 of Seqrite UTM.
10. Enter the DNS server IP address and alternate DNS server if applicable.
11. Click **Save.**

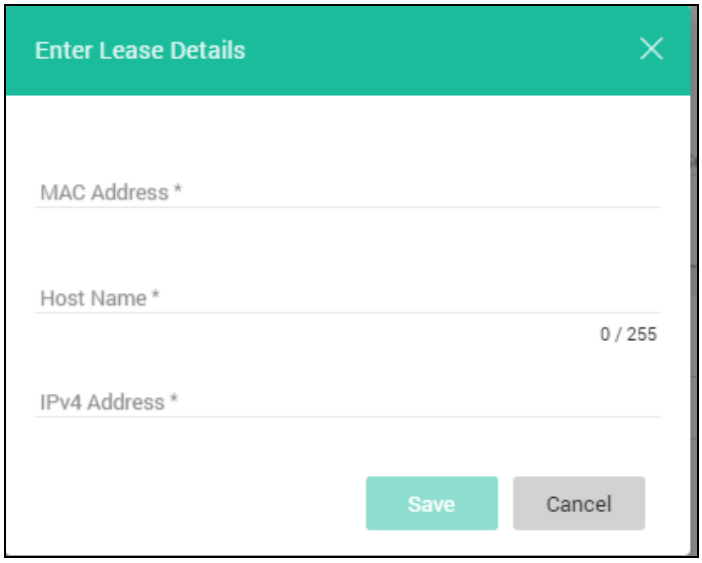
Adding Static Lease

Adding a static lease allows you to bind the IP address with MAC address of the user's computer so that only the configured IP address will be leased to the client irrespective of the other free IP addresses.

1. Navigate to **Network > DHCP > Server.**
2. Select a DHCP server from the list and click the Edit icon (seen on hover).
3. Go to the Static Lease section.



4. Click **Add** icon (+) in the **Static Lease** section.



5. Enter the following details:
    - **MAC Address**: Set the MAC address of the user's computer to which the IP address is to be bound. You can get the MAC address of client by using command "ipconfig /all" on windows client and "ifconfig" on a Linux client.
    - **Hostname**: Set the hostname of client.
    - **IPv4 Address**: Set the IPv4 address to bind. The IP address will be assigned to the user's computer. Note: This IP address must be in the local network as the Seqrite UTM.

6. Click **Save**. The static lease is added and displayed in the list. Note: Addresses in the static lease will not be displayed in the Leases list.

Deleting a DHCP server

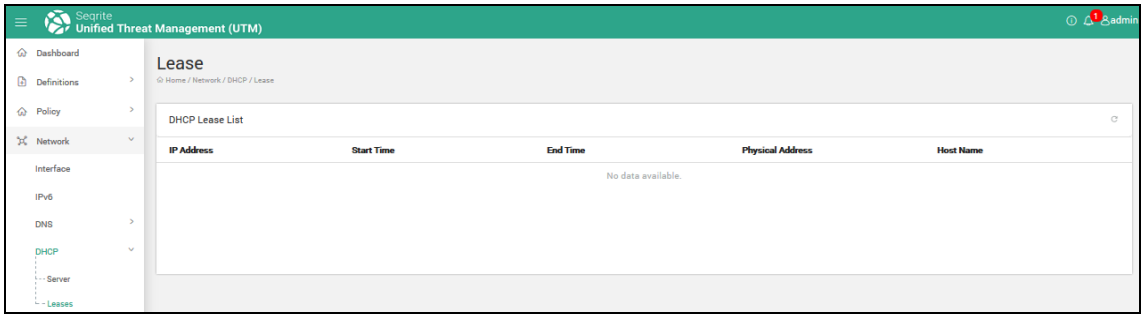
1. Navigate to **Network > DHCP > Server**. The DHCP server list is displayed that has the Server Name, Start IP address, End IP Address, Gateway IP address, DNS and a Status button.
2. Select the required DHCP Server and click the **Delete** icon on the upper right corner**.**

Viewing the DHCP Lease list

A DHCP-enabled client obtains a lease for an IP address from a DHCP server. Before the lease expires, the DHCP server must renew the lease for the client or the client must obtain a new lease. Leases are retained in the DHCP server database approximately one day after expiration. This grace period protects a client's lease in case the client and server are in different time zones, their internal clocks are not synchronized, or the client is off the network when the lease expires.

1. Navigate to **Network > DHCP > Leases**.

The list of the leased IP addresses is displayed with Lease Start Time, End Time Physical Address and Host Name that are assigned to computers in the network.

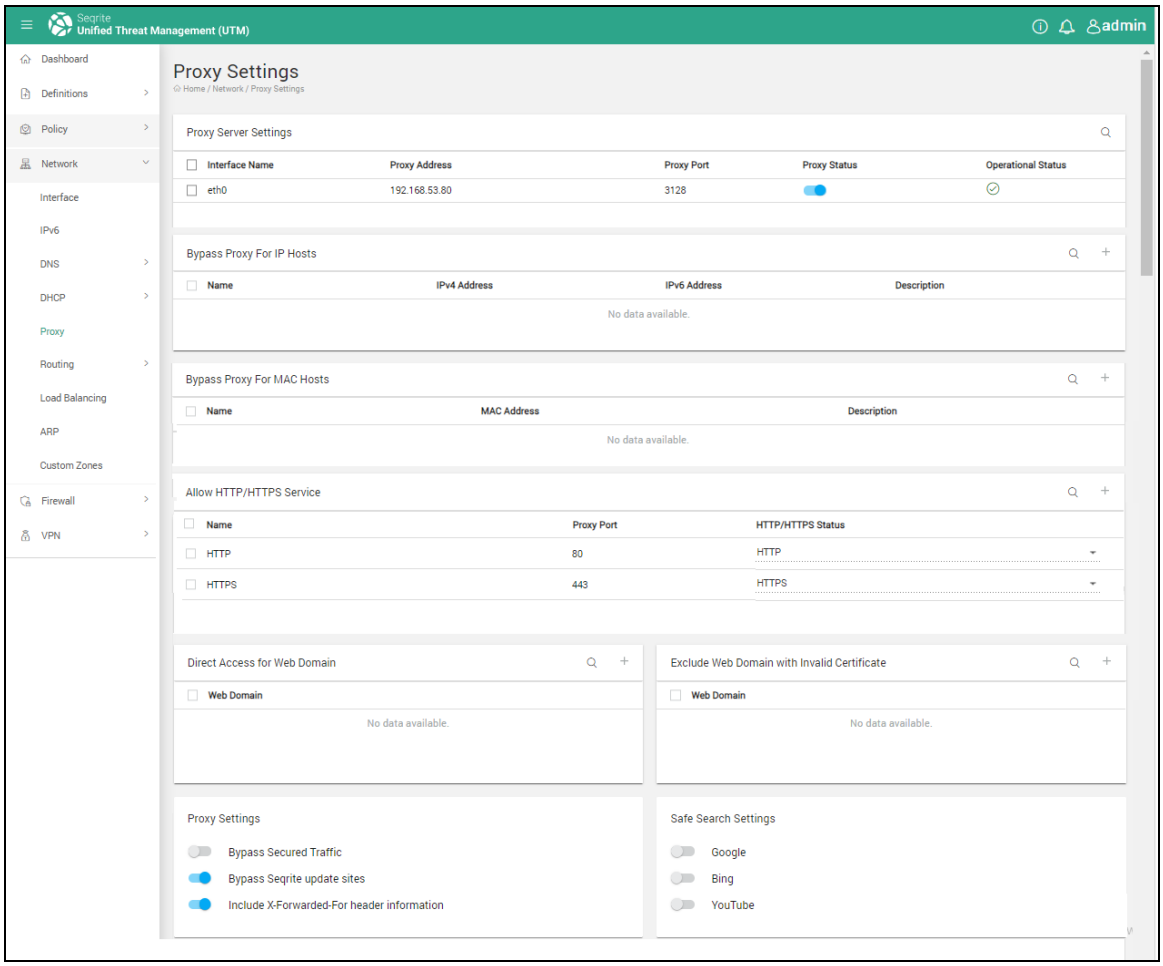


2. To refresh the list, click the **Refresh** icon on the upper right **corner.**

Proxy - Settings and Exclusion

You can control the Internet access for the user. You can give direct access or partial access depending on the designation and requirement of the user. For example, the Director or VP may require direct unfiltered content access, while others can be given access after content filtering. Also, you may not want to block the domain of your own company.

1. Navigate to **Network > Proxy**. By default, the Proxy Settings page is displayed. The Proxy Settings page displays the IP address and the ports of the Seqrite UTM.



Network Configuration

The following table describes the fields on the page, configure as required:

Field	Description
Proxy Server Settings	Displays the proxy server interface, IP address, port, and status whether enabled or disabled.
Bypass Proxy settings for Hosts	The computers in your network whose IP address is added to the Direct Internet Access list can get unfiltered access to Internet. No content or Web filtering policy is applied to the IP addresses in this list. This feature can be used for the computer/laptops of key persons, such as the Director of the company, VP, etc. so that they get unrestricted access to the Internet. You can add a single IP address or a range of IP addresses to this list. Note: You should not configure the proxy in the browser of the user.
Bypass proxy for MAC Hosts	Use this option to bypass the proxy server for specific hosts based on their MAC address.
Allow HTTP/HTTPS service	Displays the list of added services, proxy port and status of the service, whether ON or OFF.
Direct Access for web domain	Use this section to add the Web sites that should be unrestricted or need to be accessed directly without any web filtering. This feature can be used for the company's Web site.
Exclude Web domain with invalid certificate	Use this section to exclude web domains that have an invalid security certificate.
Bypass Secured traffic	Use to option to bypass all sites that are secured, i.e. URLs beginning with https.
Bypass Seqrite update sites	If you select this option, all Seqrite sites used for obtaining updates will be directly accessible without any monitoring and control. This feature allows all Seqrite UTM products deployed in the network to be silently updated.
Include X-Forwarded-For header information	To provide extra privacy to the end user, the Seqrite UTM can be configured to remove the 'X-Forwarded-For' HTTP header. By default, this option is enabled in the Seqrite UTM. Disabling this option removes the end user's host IP information from the HTTP headers in the outgoing requests. You may need to keep this option enabled especially in case of bridge mode if you are using an existing firewall.
Safe Search Settings	Enable this option to apply Safe search for Google, Bing and YouTube search results. Enabling Safe search filters out explicit content from search results.

Note: There are predefined ports, which cannot be removed. Port 80 is present under Allowed Normal Traffic by default. Similarly, Port 443 is present under Allowed Secured Traffic by default.

Configuring/Editing proxy server settings

1. Navigate to **Network > Proxy**. The Proxy server settings page is displayed with proxy interface, proxy IP address, proxy port and status.
2. Select the Proxy Interface to edit the settings. Click the **Edit** icon that is displayed when you hover. The Proxy server settings dialog box is displayed.
3. Modify the Interface name, IP address, Proxy port, and proxy status whether enabled or disabled.
4. Click **Apply**.

Routing

Routing is the process of moving data packets from one computer to another computer through a network. Routing helps in selecting the optimal path in the network to send the packets from source to destination. Routing is performed by a dedicated device called as router that forwards packets using either route information from route table entries that you manually configure.

Seqrite UTM provides features to configure the following two types of routing:

- Static Routing
- Multicast Routing
- Policy Based Routing (PBR)

Static Routing

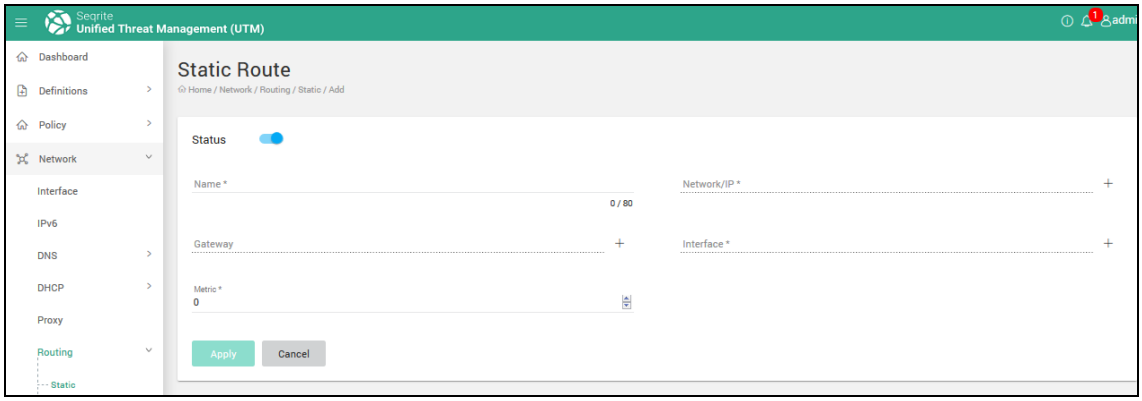
Static routing helps to define explicit paths between two routers and is not updated automatically. You must manually reconfigure the static route whenever network changes occur.

The Static Route feature on Seqrite UTM allows you to configure a route using which Seqrite UTM can use to forward the packets to a particular destination. A static route causes packets to be forwarded to a destination using a gateway other than the configured default gateway. You can add or delete the static routes or set the status from ON to Off or vice versa as required. If you set the route to OFF, then that static route is removed from the device's routing tables.

Adding a Static Route

Network Configuration

1. Navigate to **Network > Routing > Static Route**. The Static Route page is displayed which displays the list of added static routes.
2. Click the + (**Add)** icon to add a route. The following page is displayed.



3. Select the Status as **On**.
4. Enter the **Name** of the new static route.
5. Configure the destination / target IP using the Network IP field. Click **+ (Add)** to display the Network Definition list. You can browse and select or create a new Network definition using the designated icons.
6. Configure the next hop in the route using the Gateway field. Click **+ (Add)** to display the Network Definition list. You can browse and select or create a new Network definition using the designated icons.
7. Select the interface for the routing table through which you want the packets to be transmitted.
8. Enter the Metric value. Metric depicts the administrative distance for a route. Default metric for static route is 1. This value allows the router to decide a priority for a type of routing.
9. Click **Apply**. The new route is displayed in the list with the operational status.

Multicast Routing

Multicast is a technique for one-to-many communication over an IP in a network. In Multicast Routing one sender sends data to multiple known recipients. Using multicast, a source can send a single copy of data to a single multicast IP address. The data sent to this IP address is then forwarded to all the members of the associated multicast group.

Multicast uses network infrastructure efficiently by sending a packet only once, even if it has to be delivered to a large number of receivers. It saves bandwidth by sending packets only once over each link of the network.

Seqrite UTM acts as a multicast router that receives multicast data from the server and forwards it to the specified multicast group. Seqrite UTM supports the following 2 modes of multicast routing:

- Sparse mode: Sparse mode is used for transmission of data to nodes in multiple Internet domains, where it is expected that only a small proportion of the potential nodes will actually subscribe.
- Dense mode: Dense mode, in contrast to sparse mode, is used when it is expected that a large proportion of the potential nodes will subscribe to the multicast. It implicitly builds shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present.

Multicast Routing Sparse mode

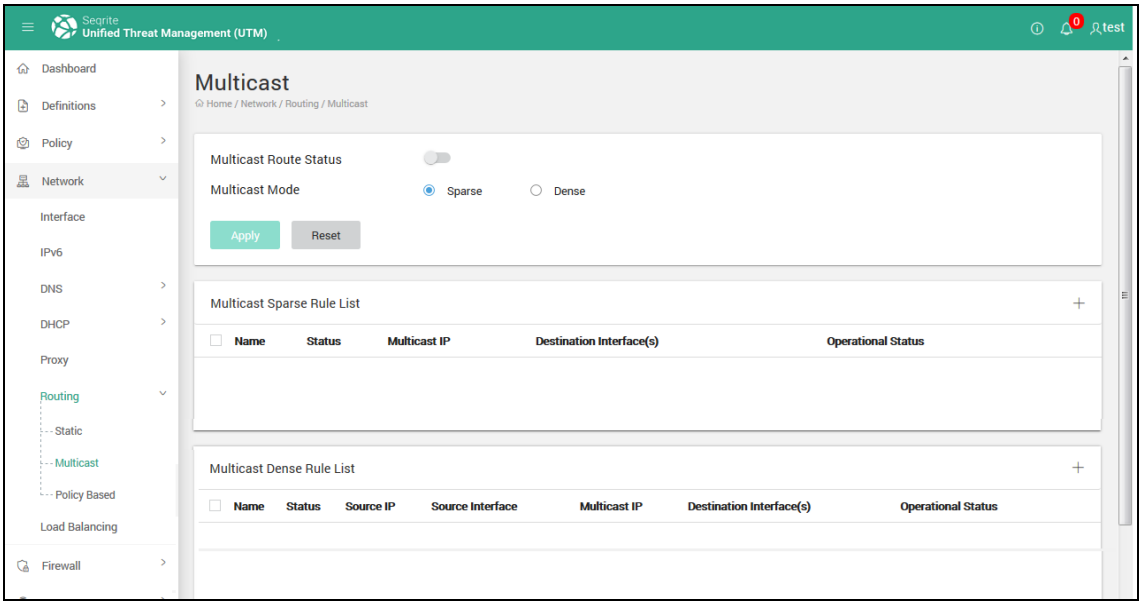
Setting up multicast routing in Sparse mode involves the following 3 steps:

1. Add a multicast route.
2. Add a custom firewall rule to open the UDP port to allow multicast traffic.
3. Add a custom firewall rule to allow the IGMP traffic from UTM to destination zone.

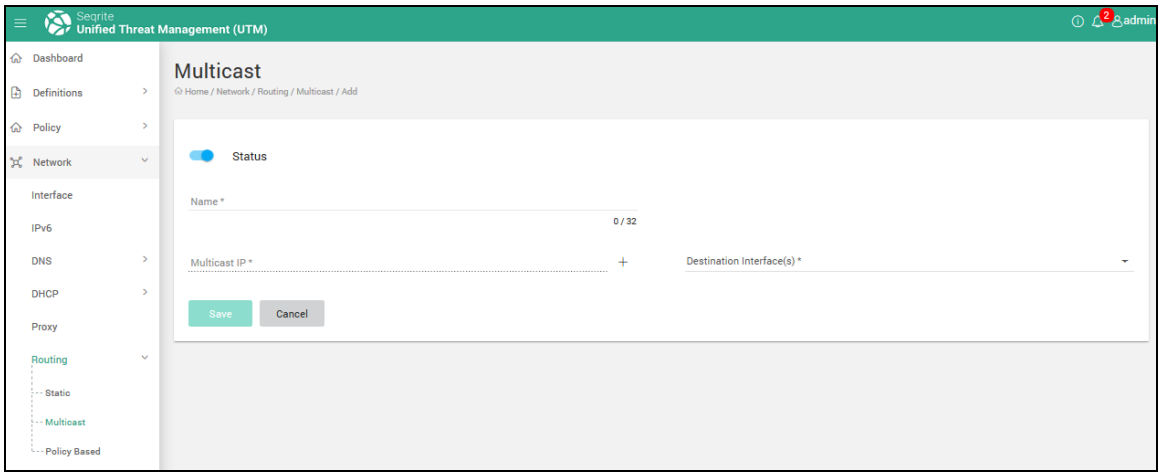
Step 1: Adding a multicast route.

To add a multicast route:

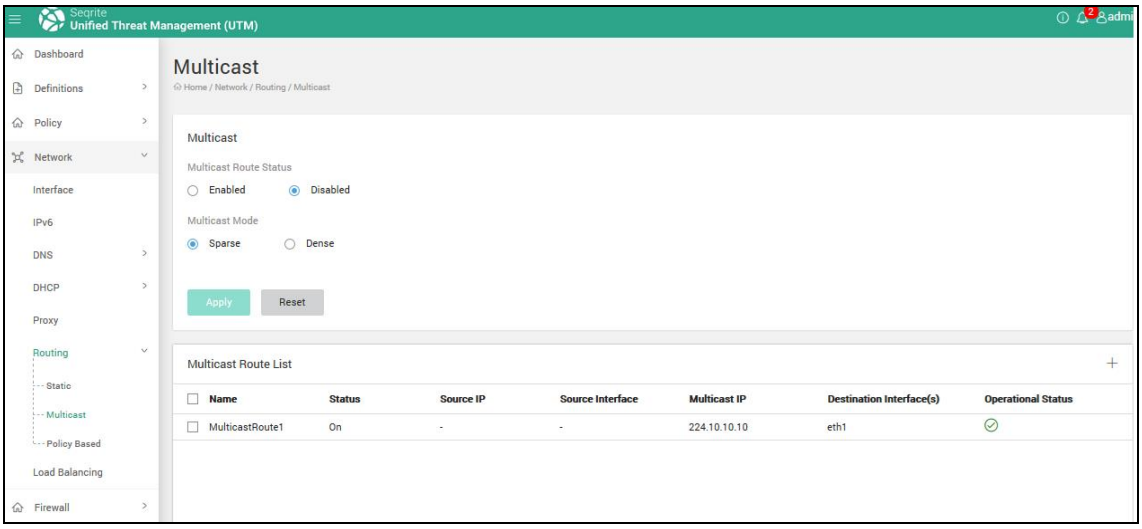
1. Navigate to **Network > Routing > Multicast.** The multicast routing list page is displayed.



2. Select the Multicast Route Status as **Enabled**.
3. Select the Multicast mode as **Sparse**.
4. Click the + (**Add)** icon in the multicast Routing list to add a multicast route in Sparse mode section. The Add multicast route page is displayed.



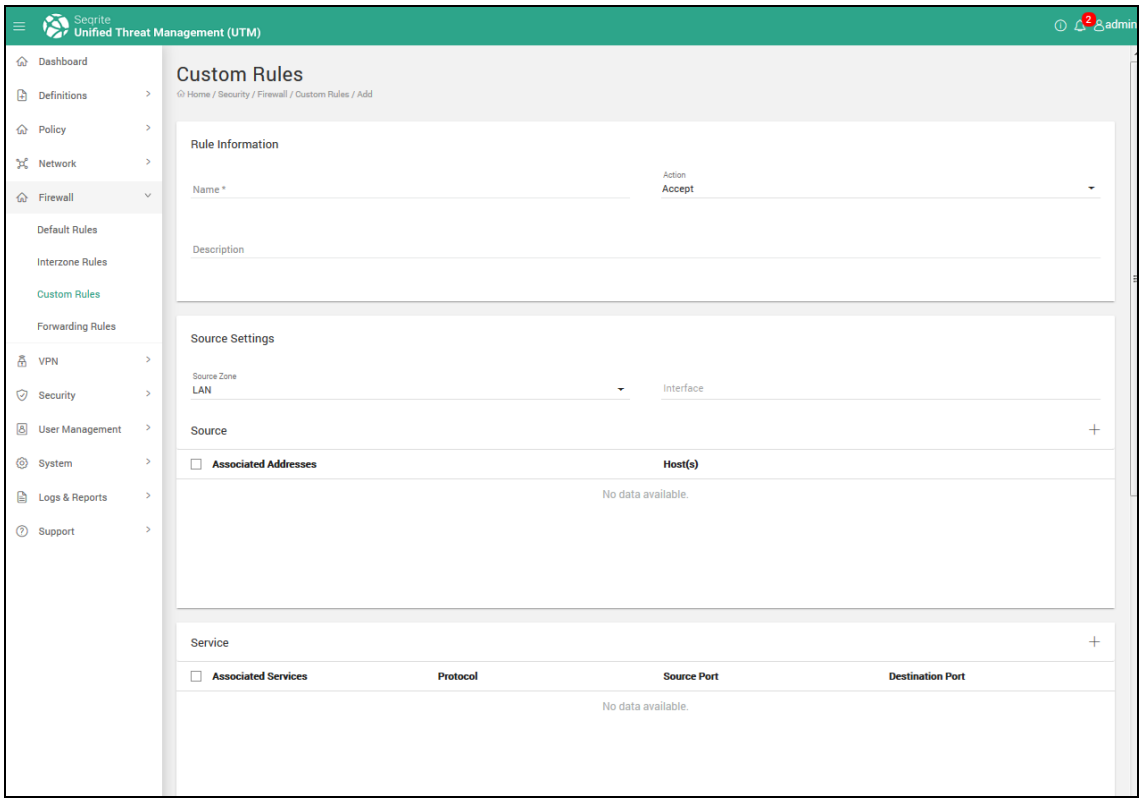
5. Enter the **Name** of the new multicast route.
6. Add the Multicast IP. This is the multicast group that will receive the data. Click on the **+ (Add)** icon. The Network definitions dialog box is displayed. You can select the Multicast IP from the list, or you can also create a new network definition. Click on Create Definition tab, enter the multicast IP details here and click Save.
   Note: You can use Network Definitions only in range of 224.0.0.0 through 239.255.255.255 as the data is multicast in nature.
7. On the Add multicast route page, select the **Destination Interface** to which the sender would multicast and through which the data will be received by the multicast group.
8. Click **Save**. The multicast route is added and displayed in the table.



Note: Hover above the multicast route and use the Edit icon to change the status of the multicast route.

Step 2: Adding a custom firewall rule to open the UDP port to allow multicast traffic.

1. Navigate to **Firewall > Custom Rules**.
2. Click the + (**Add)** icon. The Add Custom Rules page is displayed.



The following table explains the fields, configure as required.

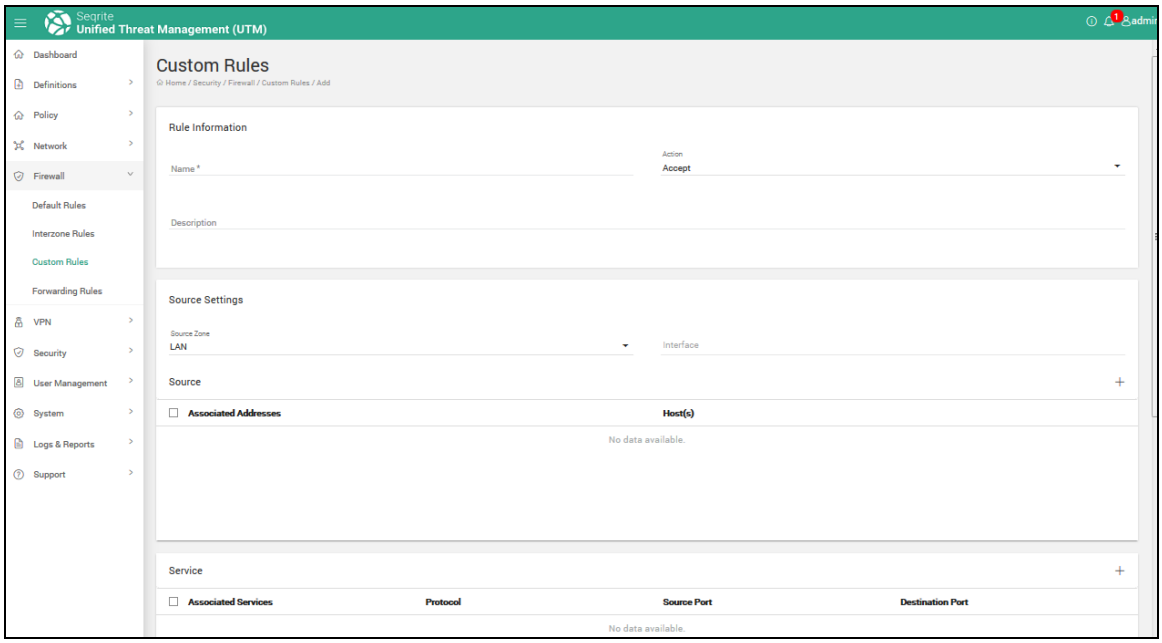
Name	Enter a Name for the custom (Multicast) rule.
Action	Select the action as Accept to allow the connection and permit the packet to traverse through the network.
Source Zone	Select appropriate source zone. Source zone list contains LAN, WAN or DMZ as options.
Source Interface	Enter the Source Interface.
Source	This is multicast sender's IP. You can browse, add or delete the Network Definition using the respective icons.
Service	This is the multicast port. Add the Service definition for multicast port. Note: While adding the service definition select the Protocol as UDP and the option for Destination port as ports and enter the value for ports as 4321.
Destination Zone	Select appropriate destination zone from the Destination Zone list. Destination zone list contains LAN, WAN or DMZ as options.

Destination Interface	Select the Destination Interface. The multicast receivers are on these interfaces.
Destination	Select the intended multicast destination address here.

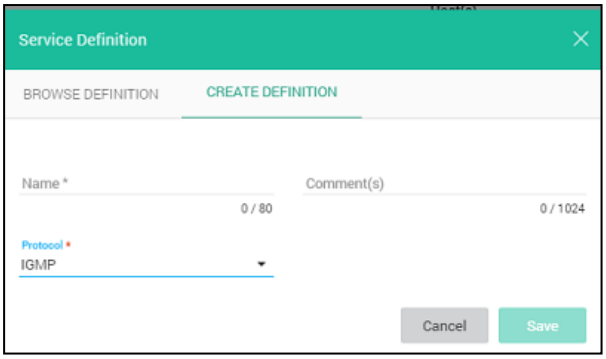
3. Click **Apply**. The rule is added in the custom firewall list.

Step 3: Add a custom firewall rule to allow the IGMP traffic from UTM to destination zone.

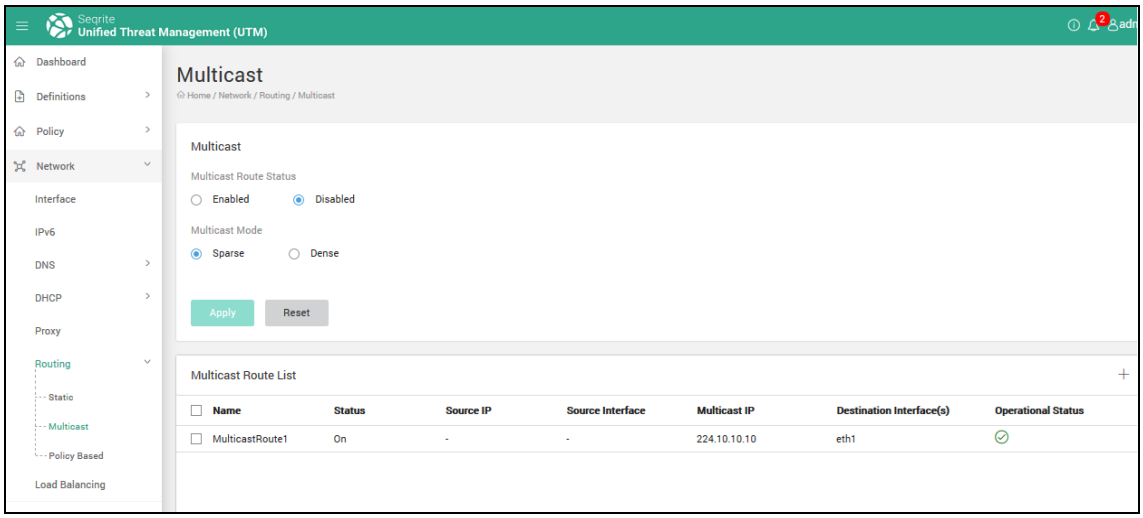
1. Navigate to **Firewall > Custom Rules**.
2. Click the + (**Add) icon**. The Add custom firewall rule page is displayed.



The following table explains the fields, configure as required.

Name	Enter a Name for the custom (IGMP) rule.
Action	Select the action as accept to allow the connection and permit the packet to traverse through the network.
Source Zone	Select the Source zone as UTM.
Source Interface	Browse and add the Network Definition 'Any IPv4'
Source	This is multicast sender's IP. You can browse, add or delete the Network Definition using the respective icons.
Service	This is the multicast port. Add the Service definition for IGMP. Browse and select the Service definition for source and  destination ports to allow IGMP traffic. If service definition does not exist, use the Create Definition option to create a service definition to allow IGMP traffic. Note: While adding the service definition select the Protocol as IGMP.
Destination Zone	Select appropriate destination zone from the Destination Zone list. Destination zone list contains LAN, WAN or DMZ as options.
Destination Interface	Select the Destination Interface. The multicast receivers are on these interfaces.
Destination	Browse and add the Network Definition 'Any IPv4'.
Advanced Settings	Select the settings as applicable for options of Active, Logging, and Apply NAT.

3. Click **Apply**. The rule is added in the multicast routing list as shown in the figure below.



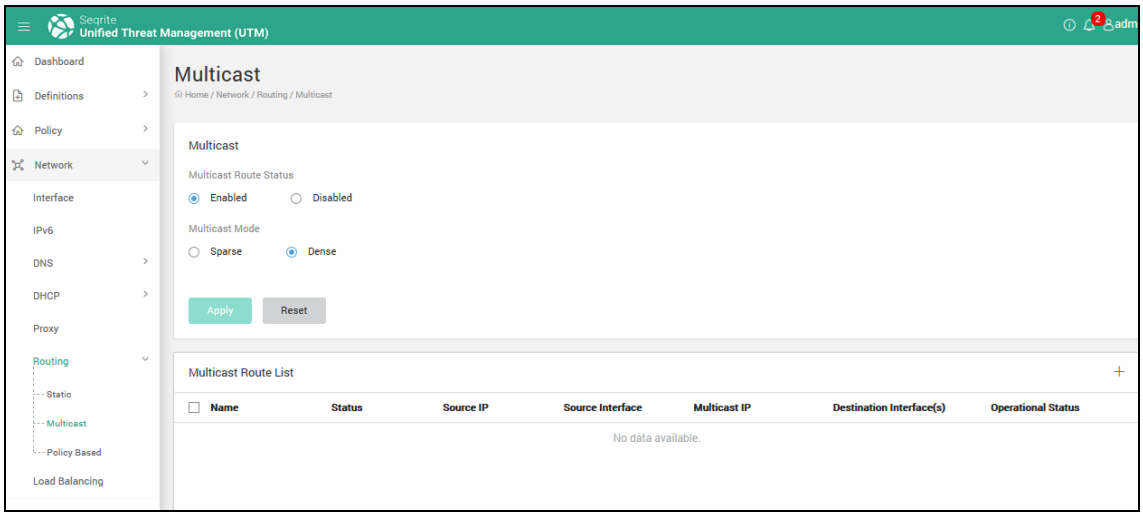
Multicast Routing Dense mode

Setting up multicast routing in Dense mode involves the following 2 steps:

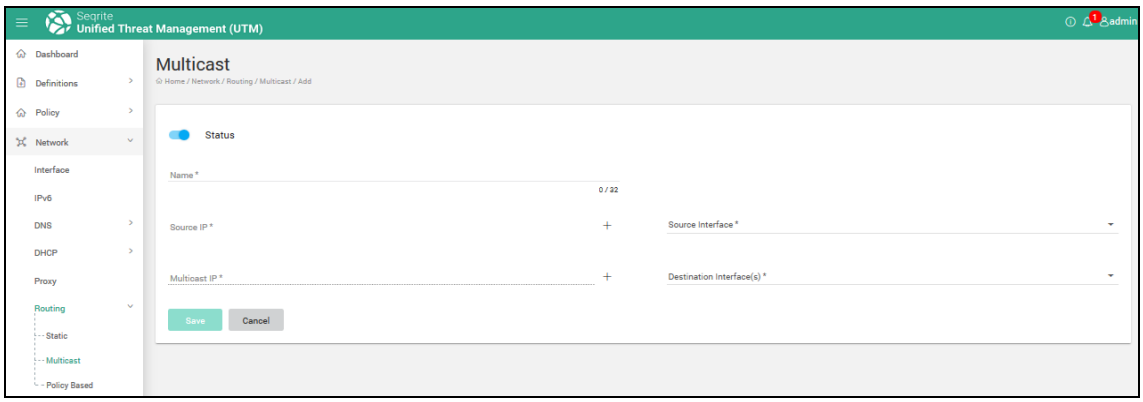
1. Add a multicast route.
2. Add a custom firewall rule to open the UDP port to allow multicast traffic.

Step 1: Adding a multicast route.

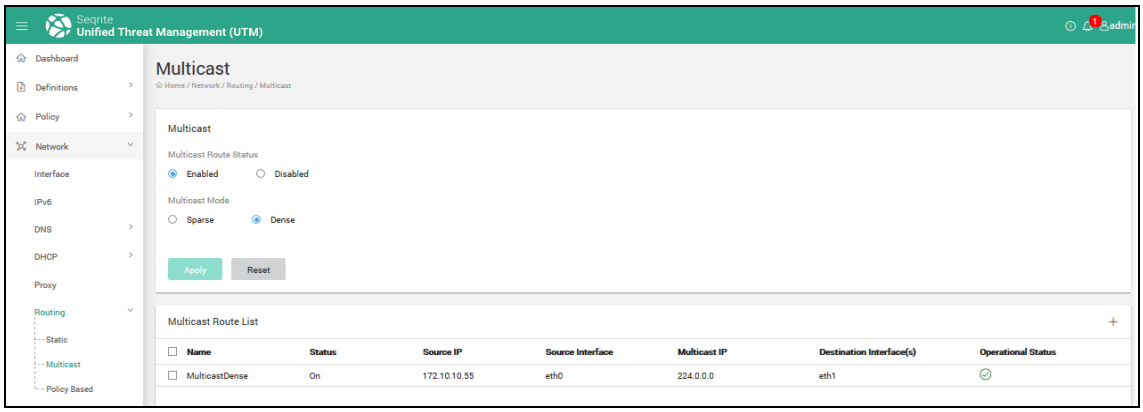
1. Navigate to **Network > Routing > Multicast Route**. The multicast routing list page is displayed.



2. Set the Multicast status as **Enabled.**
3. Select the **Multicast Mode** as **Dense**. Click on **Apply**.
4. in the Multicast Dense list, click **+ (Add)** icon to add a multicast route in dense mode. On clicking **Add**, the following page is displayed.



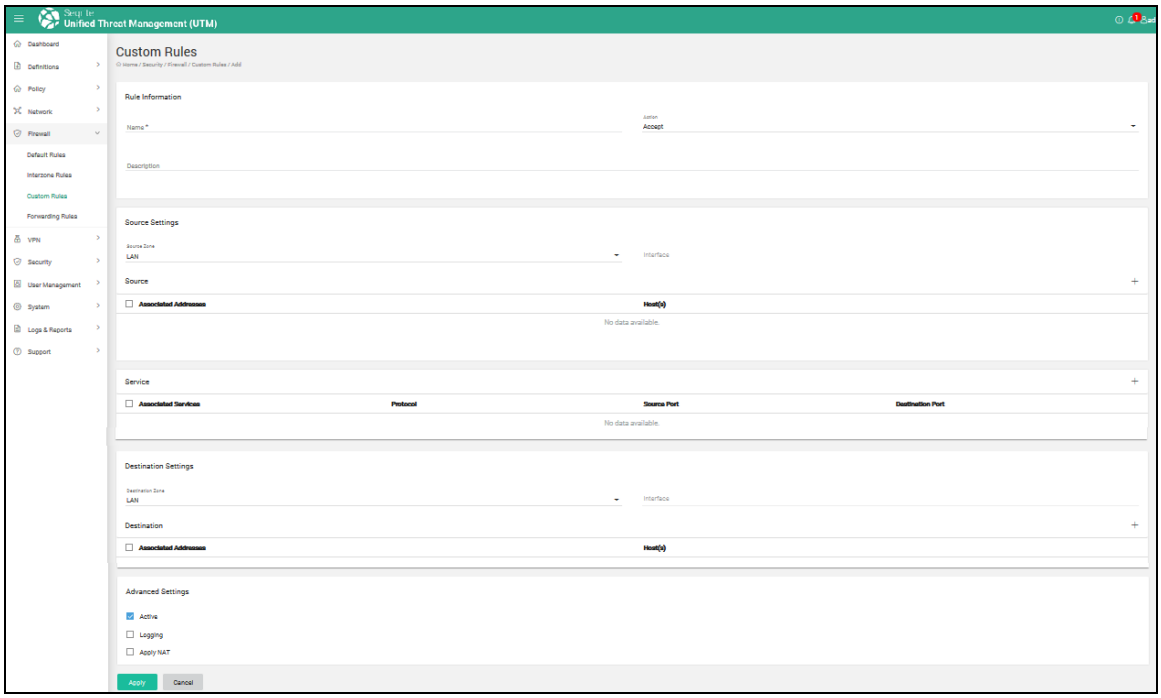
5. Enter the **Name** of the new multicast route.
6. Select the **Source Address**. This is the IP from where the multicast traffic will originate.
7. Select the **Source Interface**. This is the interface through which the multicast data is sent by the Source IP.
8. Add the Multicast IP. This is the multicast group that will receive the data. Click on the add icon (+). The Create network definition popup is displayed. Enter the multicast IP details here and click **Save**.
9. On the Add multicast route page, select the Destination Interface to which the sender would multicast and through which the data will be received by the multicast group.
10. Click **Save**. The multicast route is added and displayed in the table.



Note: You can change the status of the multicast route using the Edit button icon provided besides the **Name** column of the multicast route list.

Step 2: Adding a custom firewall rule to open the UDP port to allow multicast traffic.

1. Go to **Firewall > Custom Rules**.
2. Click on **Add**. The Custom Rules firewall rule page is displayed.



3. The following table explains the fields on the page, configure as required:

Name	Enter a Name for the Multicast rule.
Action	Select the action as accept to allow the connection and permit the packet to traverse through the network.
Description	Enter the description about the new custom rule.
Source Zone	Select appropriate source zone. Source zone list contains LAN, WAN or DMZ as options
Source Interface	Enter the Source Interface.
Source	This is multicast sender's IP. You can browse, add or delete the Network Definition using the respective icons.
Service	This is the multicast port. Add the Service definition for multicast port. Note: While adding the service definition select the Protocol as UDP and the option for Destination port as ports and enter the value for ports as 4321.
Destination Zone	Select appropriate destination zone from the Destination Zone list. Destination zone list contains LAN, WAN or DMZ as options.
Destination	Select the Destination Interface. The multicast receivers are on these

Interface	interfaces.
Destination	Select the intended multicast address here.
Advanced Settings	Active: BY default, the rule is active after you create it. You can choose to render it in-active by remove the checkbox. Select the Logging check box to enable logging of the changes to Interzone firewall rules. Select the settings as applicable for options of Active, Logging, and Apply NAT.

4. Click **Apply**. The rule is added in the custom firewall list.

Policy Based Routing (PBR)

PBR helps you in routing packets as per the defined policy for the traffic flow. You can use PBR if you want certain packets to be routed through a way other than the optimal path. It also allows you to specify a path for certain traffic and route packets based on company policies. For example, you can implement routing policies to allow or deny paths based on the identity of a particular end system, an application protocol, or the size of packets.

The PBR feature on Seqrite UTM helps you to create policies to configure traffic to be routed as per defined criteria for the interfaces. The routing can be based on the following:

- Source type
- Source interface
- Service-based
- Destination

If network traffic passing through Seqrite UTM satisfies the provided criteria, traffic will be forwarded through a target network interface link or target gateway.

The PBR criteria can be a combination of source network interface, source IP address/source network/user/group, service, time category and destination network. Thus, PBR allows to the administrator to differentiate traffic based on various filters rather than just destination IP address in packet, thereby providing granular control over network traffic.

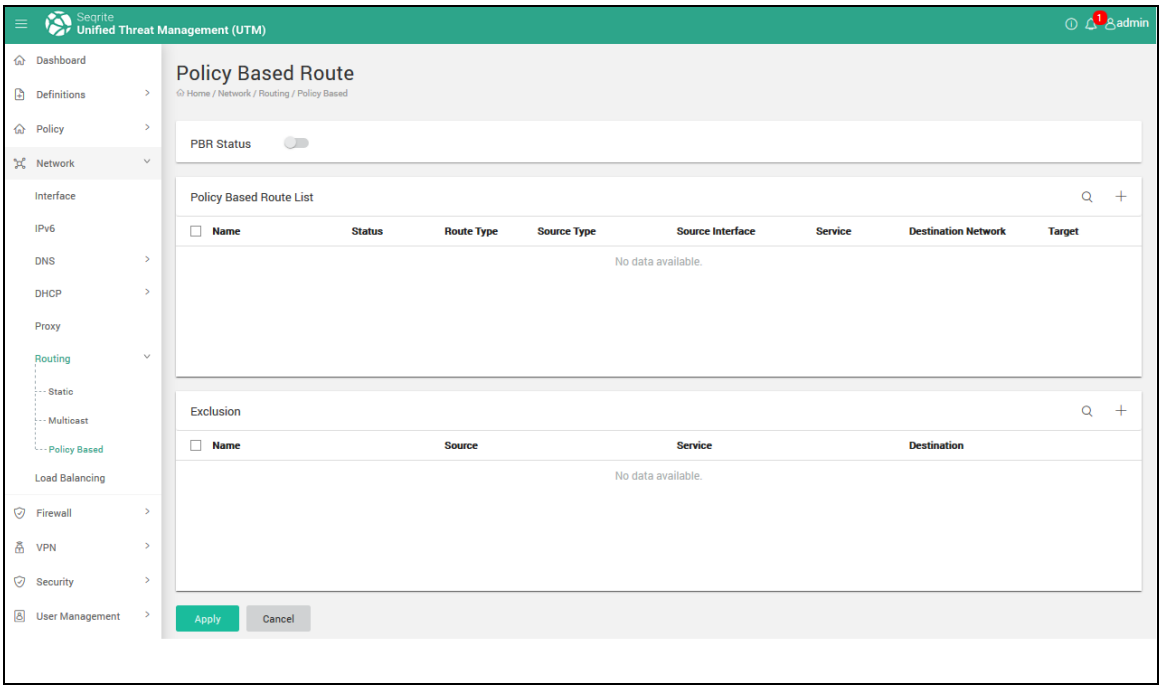
Enabling PBR

1. Navigate **to Network > Routing > Policy Based**.
2. Toggle the status button to enable the PBR status.
3. Click **Save**.

Adding routing policies

1. Navigate to **Network > Routing > Policy Based**.

2. Click **Add**. The following page is displayed.



3. The following table describes the fields on the page, configure as required.

Field	Description
Name	Unique Policy Based Route rule name which is used to identify the rule.
Position	Each Policy Based Route rule will have a position among all Policy Based Route rules. Rules will be applied based on their position. So, rule at the first position in the list will be applied first to the network traffic, if this rule satisfies the criteria traffic will be forwarded to Target network Interface as mentioned in the rule. If first rule is not applicable, then the next rule will be applied. This process will be continued till the last Policy Based Routing rule.
Source Interface	All local network interfaces (LAN, DMZ, LAN-LAN network bridge interface, LA interface) will be listed in here. One or more or any source network interfaces can be selected from the list. This is the interface from where the packets are coming.
Source Type	Policy Based Route rule can be applied on Users, Group, IP Address, IP Address Range, and Network definitions. Select one of these types.
Source	Displays the list according to the source type selected. Select the Source.
Service	Select Service definitions for which this rule should be applicable. Service is identified based in source port or destination port or both. (See **Definitions** for more details of Service Definition).
Route Type	Route Type can either be Interface Route or Gateway Route. If network traffic has to be forwarded through a network interface, Interface Route option should be selected. Only WAN interfaces are listed in Interface route. Gateway Route can be selected, if network traffic has to be transferred to a gateway (IP Address) reachable from any one of the configured network interfaces. Only Hosts are displayed in the list.
Target	Target can either be a network interface or a gateway based on Route Type. If Target is not active, then traffic will be forwarded through default system routing decision. Displays the list based on the Route Type selected.
Time Category	Select respective time category(s), if Policy Based Routing rule is to be effective for a specific time. If Time Category is not selected, it will be

Field	Description
	set to Default time category.
Destination Network	This is the destination where the packets are forwarded. Traffic can be forwarded based on the destination network. If not selected, any destination network will be considered. Only list of Network definitions is displayed. (See **Definitions** for more details of Network Definition)

3. Make the required changes and click **Apply**.

Deleting a routing policy

1. Navigate to **Network > Routing**.
2. Select the policy that you want to delete and click **Delete.**
3. Click **OK** on the confirmation box. The policy is deleted.

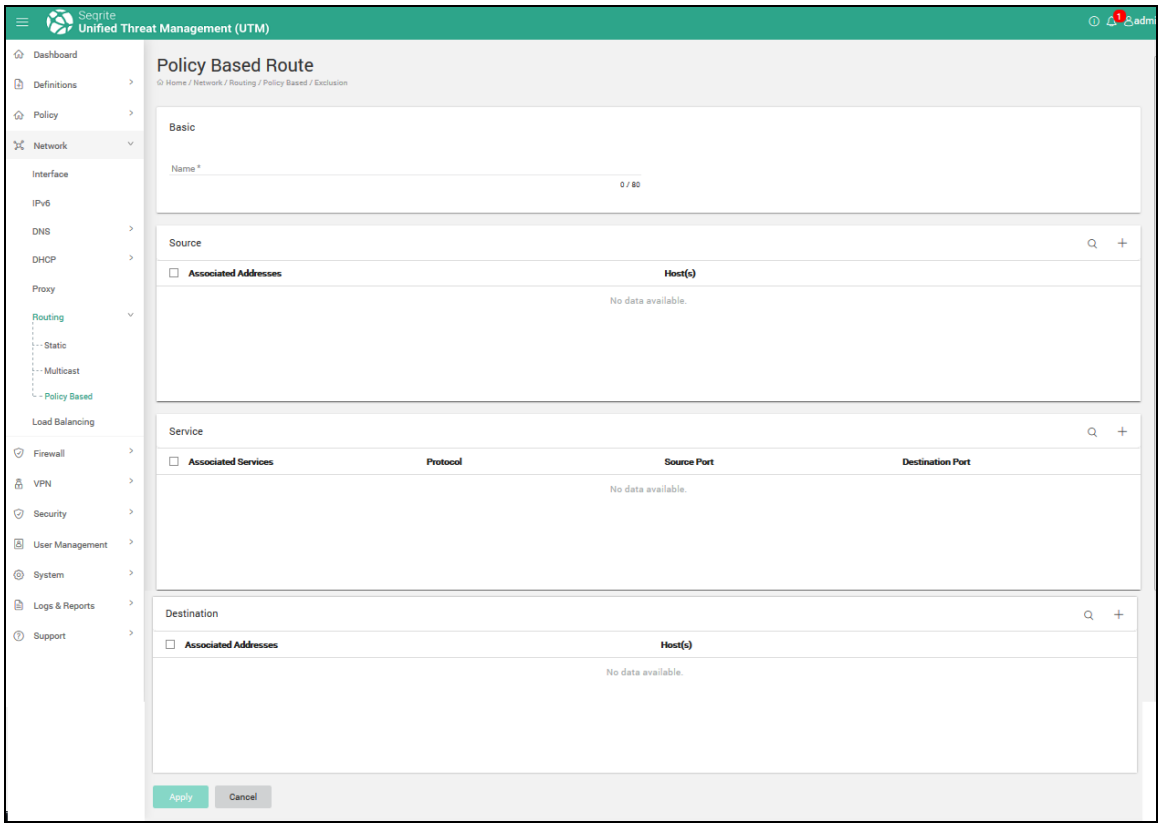
Changing the priority of policies

1. Navigate to **Network > Routing.**
2. Click the type, whether Static, Multicast or Policy Based. The corresponding policy list is displayed.
3. Select the policy for which you want to change the priority, click the **Change Priority** arrows, up or down as required to change the priority.
4. Click **Save**.

Adding exclusions to PBR

You can exclude a network traffic from the Policy Based Routing rules using the Exclusion section on the PBR list page. You can add a criterion in Policy Based Route Exclusion for this network traffic.

1. Navigate to **Network> Routing**> **Policy Based**.
2. Click + **(Add)** in the **Exclusion** section. The following page is displayed.



3. In the Basic section, enter the unique **Name** for exclusion.
4. Select **Source definition**(s) the by browsing, adding or deleting unwanted definitions using the icons provided.
5. Select **Service definition**(s) using the icons provided.
6. Select the **Destination Network** by browsing, adding or deleting unwanted definitions using the icons provided.
7. Click **Apply**.

Dynamic Routing

Dynamic routing is a networking technique that helps the routers choose the most optimal path to route data packets based on real-time logical network layout changes.

Seqrite UTM supports the popular protocols BGP and OSPF. These routing protocols enable the routers exchange routing information by which, the routers dynamically learn about the shortest path to remote hosts. This information is then added to their routing tables as a basis for forwarding packets.

Seqrite UTM provides features to configure the following two types of dynamic routing:

- Routing using BGP protocol
- Routing using OSPF protocol

You need to do the following for dynamic routing to work:

- Configure Interfaces.
- Create Firewall rules.
- Create Users who will be using the dynamic routing.

Dynamic Routing using BGP protocol

Border Gateway Protocol (BGP) protocol generally used by ISPs contains network path information which enables the routers to share routing information between autonomous systems (AS) so that optimal routes can be used. A connected group of networks or routers that are controlled by a single administrative entity and share common routing policies can be called an autonomous system. An AS is identified by a unique AS number.

This AS number helps share routing information between neighboring AS. Use private AS numbers from 64512 to 65535 if a unique AS number is not required.

BGP dynamic routing enables advertisement of self-service (private) network prefixes to physical network devices that support BGP such as routers. BGP relies on address scopes and requires knowledge of their operation for proper deployment.

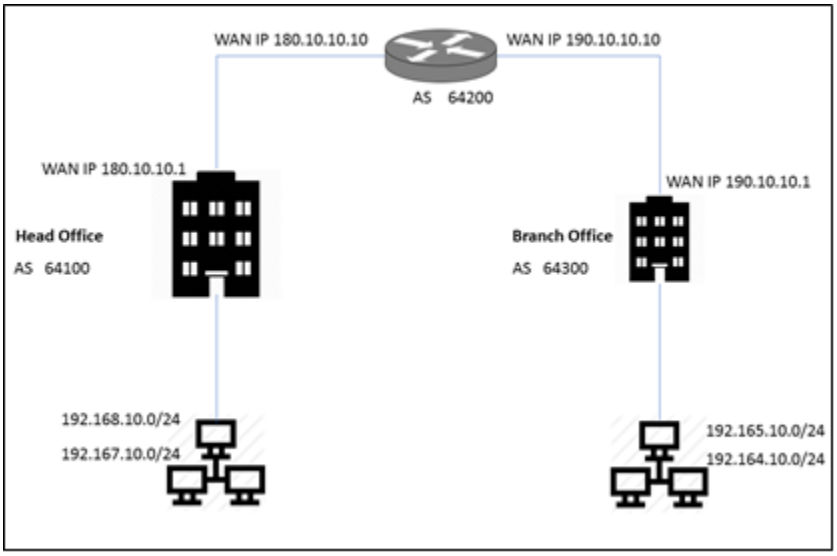
BGP selects a single path from the multiple advertisements received from multiple sources, puts it in the IP routing table and passes the path to its neighboring AS.

Pre-requisites to using BGP in your network

1. If the interface zones are created as LAN, then you have to create custom firewall rule LAN-LAN with NAT.
2. If the interface zones are created as WAN, then you have to create LAN to WAN Interzone rules as by default NATting is applied on WAN rule.
3. For BGP configuration, OSPF must be configured for IBGP to work because OSPF works as a carrier for IBGP.

Network Architecture diagram for using BGP routing

Use Case: Your Head office and Branch office are geographically located at a distance or in a separate city. To be able to connect your intranet securely across both offices, you can use the BGP protocol.



Head office configuration

1. Navigate to Network > Routing > BGP.
2. Toggle the BGP status button to enable the dynamic routing using BGP.
3. Enter the Router ID of the ISP border router. The router ID helps identify a BGP router. It is usually the IP address of the gateway. You can obtain this from your ISP. For above configuration, router ID is 180.10.10.1
4. Enter the local Autonomous Number (AS) number of your internal router (in this case for the Head Office). AS may be a number from range: 1 to 4294967295. For above configuration AS is 64100.

5. Add the neighbors (in this case your ISP) IPv4 address and AS details as required. The neighbors are the related AS systems. For above configuration IP address is 180.10.10.10 and the AS is 64200.
6. Add the network and the subnet masks of your internal network as required. The BGP protocol will advertise these networks. In above configuration, network IP is 192.165.10.0 and subnet mask is /24 (255.255.255.0) 192.164.10.0 and subnet mask is /24 (255.255.255.0).
7. Click **Apply**.

Branch Office configuration

1. Navigate to Network > Routing > BGP.
2. Toggle the BGP status button to enable the dynamic routing using BGP.
3. Enter the Router ID of the ISP border router. The router ID helps identify a BGP router. It is usually the IP address of the gateway. You can obtain this from your ISP. For above configuration, router ID is 190.10.10.1
4. Enter the local Autonomous Number (AS) number of your internal router (in this case for the Head Office). AS may be a number from range: 1 to 4294967295. For above configuration AS is 64300.
5. Add the neighbors (in this case your ISP) IPv4 address and AS details as required. The neighbors are the related AS systems. For above configuration IP address is 190.10.10.10 and the AS is 64200.
6. Add the network and the subnet masks of your internal network as required. The BGP protocol will advertise these networks. In above configuration, network IP is 192.168.10.0 and subnet mask is /24 (255.255.255.0) 192.167.10.0 and subnet mask is /24 (255.255.255.0).
7. Click **Apply**.

Dynamic routing using OSPF

OSPF routing protocol calculates the shortest route to a destination through the network based on the cost of the route, considering bandwidth, delay and load. The administrator decides the weightage of the various parameters.

All routers in an OSPF network continuously update their link state databases with information about the network topology and adjust their routing tables. An OSPF network can be subdivided, into routing areas. An area is a set of routers that are administratively configured to exchange link-state information with each other. Areas help simplify administration and optimize network traffic utilization.

Areas are identified by 32-bit numbers that are similar to the same dot-decimal notation used for IPv4 addresses. You can also set the IP address of a main router in an area as the area identifier. All additional area must have a connection to the main OSPF area. These connections are maintained by the area border router (ABR) which is an interconnecting router.

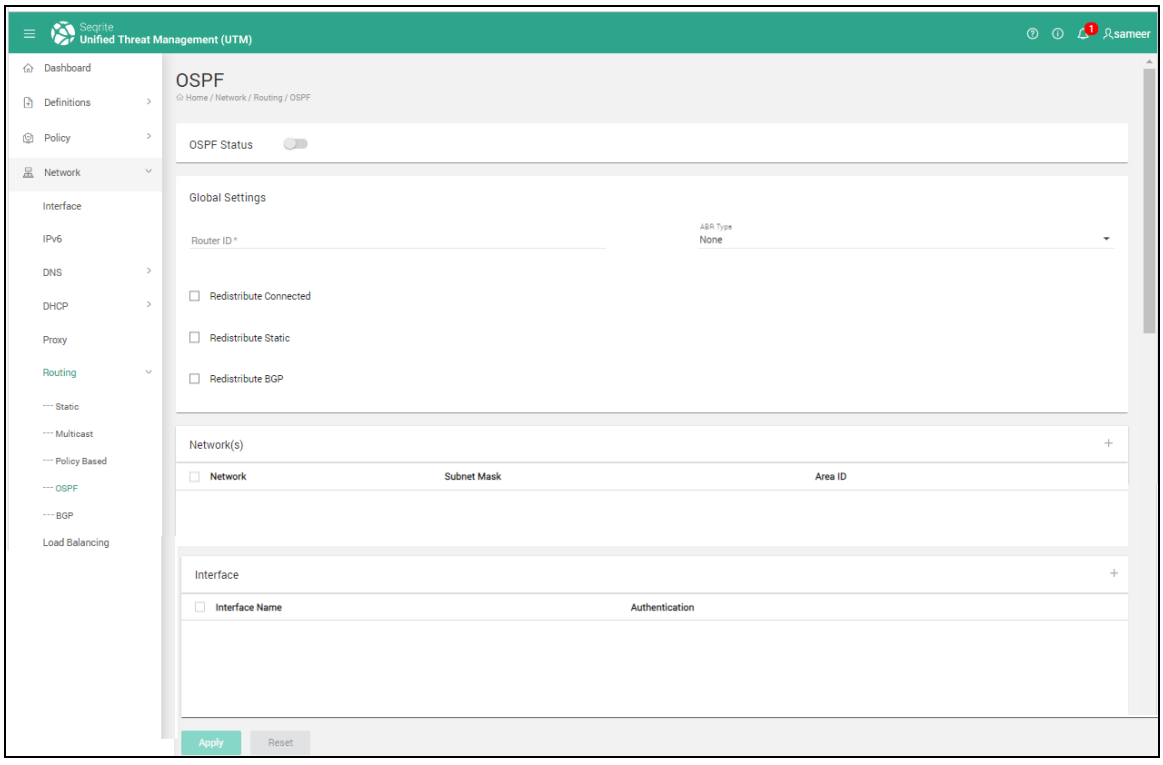
The ABR maintains unique individual link-state databases for each area. It also keeps a table of summarized routes for all areas in the network. OSPF detects any link failure or changes in the topology and instantly switches on a new loop-free routing structure within seconds.

Pre-requisites to using OSPF in your network

1. If the interfaces are created as LAN, then you have to create LAN to LAN interzone rules. Else LAN to WAN interzone rules should be created for WAN zone.
2. In case of REDISTRBUTION of routes in OSPF; which will be treated as external routes (E2/E1) within OSPF, you need to apply LAN-LAN with NATing rule on UTM which is doing redistribution.
3. Create the users for the networks for which the traffic is getting forwarded through the UTM.

To use OSPF-based dynamic routing in UTM follow these steps:

1. Navigate to **Network > Routing > OSPF**.
2. Toggle the OSPF status button to enable the feature.



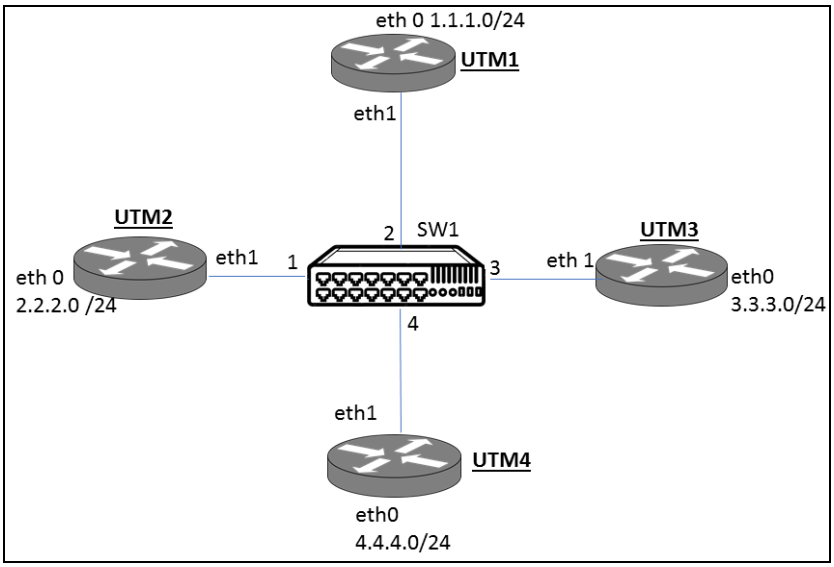
3. In the Global settings area, enter the Router ID and ABR type.

4. Select the type of route redistribution, whether Redistribute connected, or Redistribute static or Redistribute BGP depending on your network topology.
    - Redistribute Connected Routes: Use this option to redistribute the routes learnt from one of your interfaces that is configured with OSPF with your other directly connected interfaces that are not configured with OSPF.
    - Redistribute static routes: Use this option to redistribute the routes learnt from static routing protocol into interface with OSPF.
    - Redistribute BGP: Use this option to redistribute the routes learnt from BGP routing protocol into interface with OSPF.
5. In the Networks area, click + to add the networks that you want to connect using OSPF. Enter the network IP, subnet mask, and area ID. Note: The area ID must be in the format x.x.x.x. E.g. For an area 0, it may be in the format 0.0.0 0.
6. Click **Save.**
7. In the Area section, enter the area ID, select the area type, virtual link and the Authentication type. whether text or MD5.
8. In the Interface section, enter the interface details.
9. Click **Apply**.

Sample topology for using OSPF

In the following topology, 4 different UTM appliances within your internal network are shown. Through a common switch SW1, these appliances communicate with each other.

Network Configuration



1. Enable OSPF on UTM 1 and enter the router ID for UTM1 on the OSPF page.
2. Select the ABR type as required.
3. Select the Redistribute options as required.
4. In the Network section, add the network IP and Interfaces override information for eth0 and eth1 interfaces of UTM1.
5. Click **Apply**.
6. Repeat above procedure for UTM 2, UTM 3 and UTM 4 and configure OSPF on both interfaces as required Note: For above example, as all UTMS are in same area. use common area, if in a different area, configure accordingly.

Load Balancing and Failover

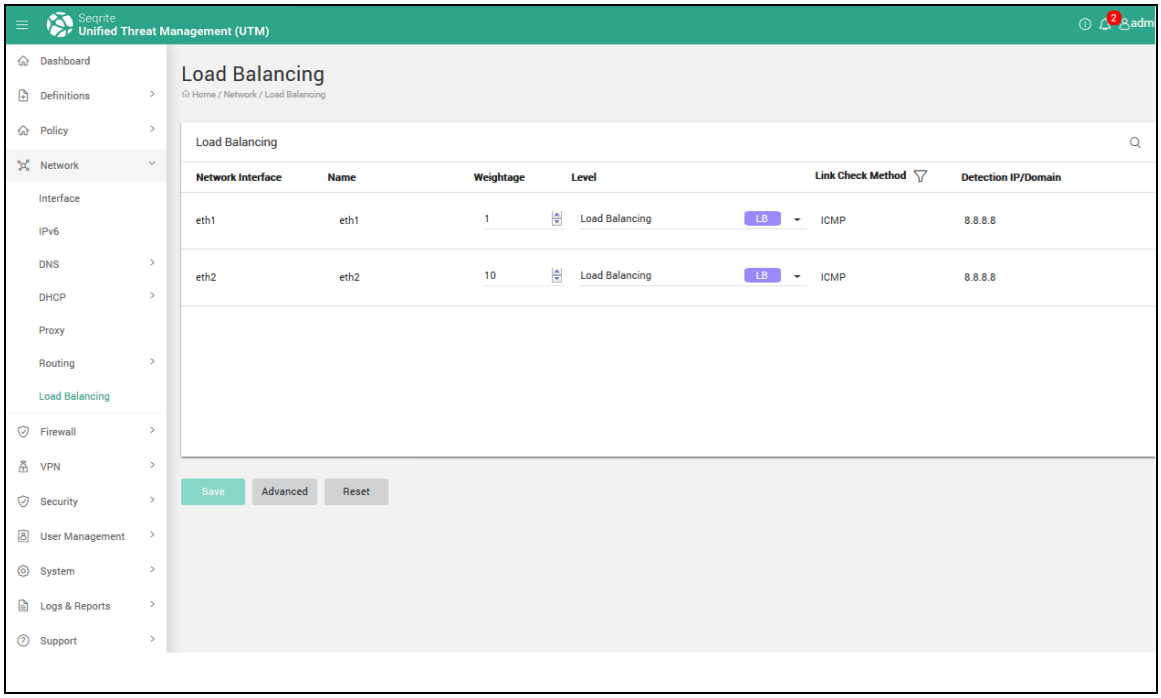
Load balancing helps in balancing the Internet traffic in case you have more than one Internet connections. You can set the weightage for the Internet connections which helps to describe the amount of traffic that will pass through the respective WAN interface. Higher the weightage more traffic is allowed through that WAN interface. You can also set the priority of the WAN interface that defines which interface will be used initially for the network connection establishment. The topmost interface in the table has the highest priority. Thus, load balancing helps in achieving optimized utilization of all links, distributed network traffic and improved user performance without overburdening any links.

Seqrite UTM also provides the failover feature in which if any link is down /unavailable then the traffic will be diverted through the other link which is active. This helps the user to get an uninterrupted Internet connectivity.

Note: If Load balancing option is enabled, then no interface can be configured as default interface.

Configuring Load balancing/Failover

1. Navigate to **Network > Load Balancing**. The Load Balancing screen is displayed with the list of the configured interfaces connected to the Internet.



2. Enter the Weightage value for each interface. Weightage decides the amount of traffic that will be sent through the interface. For example: if there are 2 interfaces eth1 and eth2 with weightage 1 and 10 respectively, then during load balancing most of the traffic will be sent through eth 2 which has weightage as 10.

   Note: By default, the Weightage is one. You can enter a value less than or equal to 99.

3. Select the Level for the interface as load balance. The following levels are available:

   i. **Default Route**: Select this option if you want to set the interface as default route.

   ii. **Load Balancing**: Select this option if you want the interface to participate in load balancing. You need to select this option for at least 2 interfaces for load balance to work.

   iii. **Failover**: Select this option if you want to set the interface for failover.

   iv. **Not a participant**: Select his option if you do not want the interface to be a participant in load balance or failover.

   You can also add new levels for failover. Depending on the failover level the interface will be up during failover.

4. Confirm the link check method and Detection IP. The link check methods check if the interface is up and connected. You can configure the method as ICMP or DNS. The Seqrite UTM pings the configured DNS or IP to check if the interface is up and connected.

5. If you want to configure the Advanced options, click **Advanced**. Configure the failover check time, WAN interface, Number of tries, Number of success, and Receive timeout duration.

Note: It is recommended to use the default values. If you configure a higher number of tries or a high number of success, Seqrite UTM might experience a degradation in performance.

Working: Seqrite UTM will periodically check the configured WAN interfaces for connectivity as per specified duration in Failover check time using the configured Link check method for that interface.

The value specified for number of tries is number of ping/lookup attempts to check WAN connectivity using the configured link check method for that interface. The number of success value is the number of successful attempts that must result from the ping/lookup attempts (number of tries) to maintain the interface as valid for load balancing.
The ratio of the number of tries to the number of success decides if the interface is valid for load balancing. If the successful ping/lookup attempts is less than the defined value under " Number of success", the interface is rendered invalid for load balancing till the next round of attempts to check connectivity which repeats after the duration specified in Failover Check time.
For e.g. If the number of tries is specified as 5, and the Number of success if set at 3, any value of successful attempts less than 3 will render the interface invalid for load balancing till the next check attempt.
The 'Receive time' out in secs and millisecs is the duration that Seqrite UTM will wait for response between consecutive ping/lookup attempts. If the ping/lookup attempt is successful as per the ratio defined for number of tries to number of success, further attempts to check connectivity are abandoned and interface is held valid for load balancing till the next round as defined by Failover Check time.

6. Click **Save**.

ARP

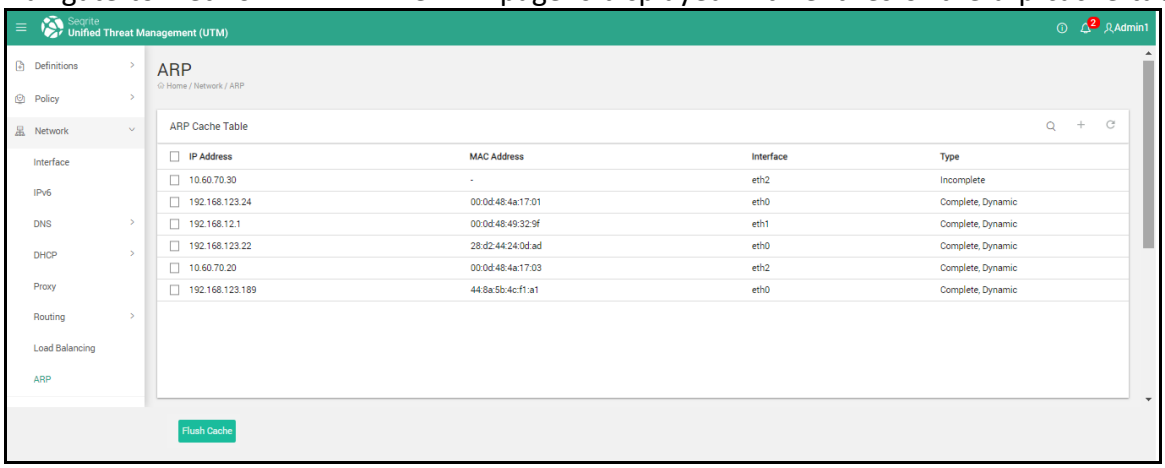
Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address (MAC) that is recognized in the local network. In the UTM appliance, the ARP cache table is displayed on the ARP page under the Network section. The following information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

Viewing the ARP cache table

1. Navigate to Network > ARP. The ARP page is displayed with entries of the arp cache table.

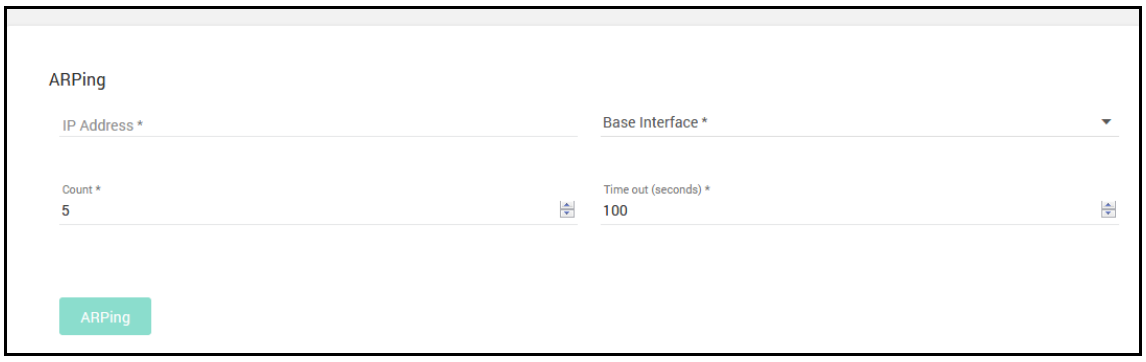


2. To flush the entries of the ARP cache table, click **Flush Cache**. The table will be cleared, and the entries refreshed.

Running the ARPing utility

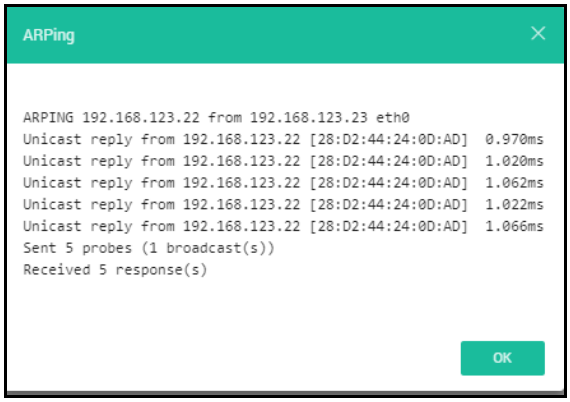
The ARPing utility on the UTM appliance lets you probe peer devices on your network. You can run the ARPing utility for a device by entering the IP address and the corresponding connected interface and obtain the MAC address of that particular device.

1. Navigate to **Network > ARP**. Scroll down to the ARPing section.



2. Enter the IP address of the device that you want to get the MAC ID, the interface on which the device is connected, the count and the timeout duration.

3. Click ARPing. The result is displayed as follows:

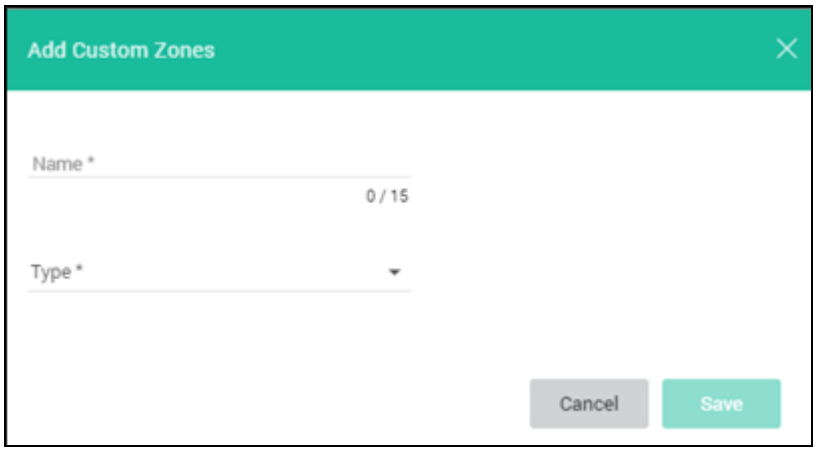


4. Click **OK** to close the ARPing dialog box.

Custom Zones

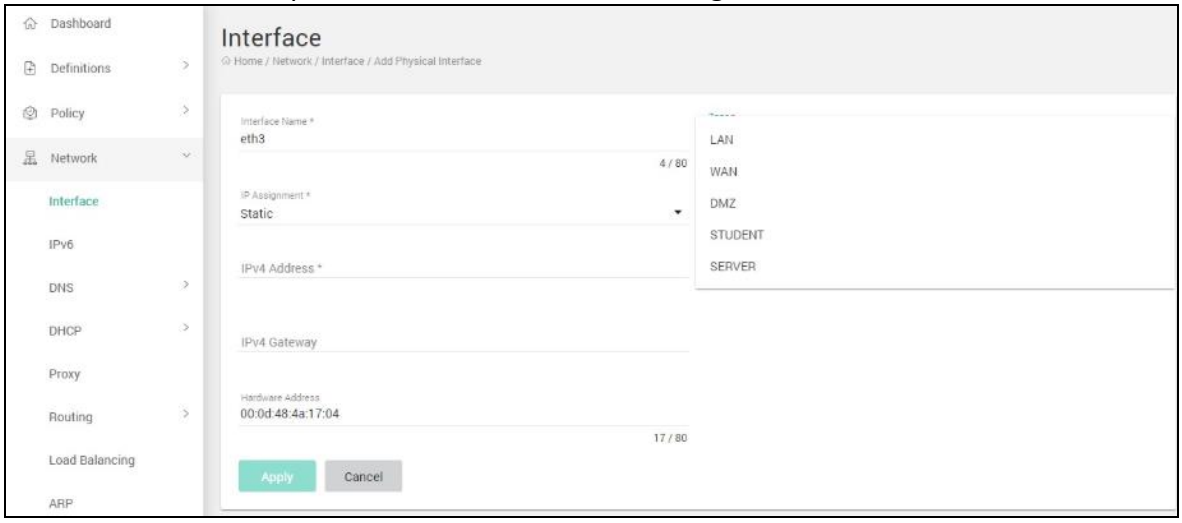
A network zone is a physical or a logical network such LAN, WAN and DMZ. Similar to these zones, you can create a custom zone in Seqrite UTM which will be treated as an entirely different subnetwork zone. You can create a LAN or DMZ type custom zone, which can be assigned to a network interface. After configuring the custom zone on a network interface, you can create custom firewall rules exclusively for that custom zone.

1. Navigate to Network > Custom Zones.
2. In the Custom Zones area, click + (Add) to add a new custom zone. The Add custom zone dialog appears.



3. Enter the name and select zone type, whether LAN or DMZ.
4. Click Save. The zone is saved, and custom zone list updated.

You can apply the custom zone to an interface while adding an interface by selecting the zone from the drop down as shown in the following screenshot:



Link Aggregation

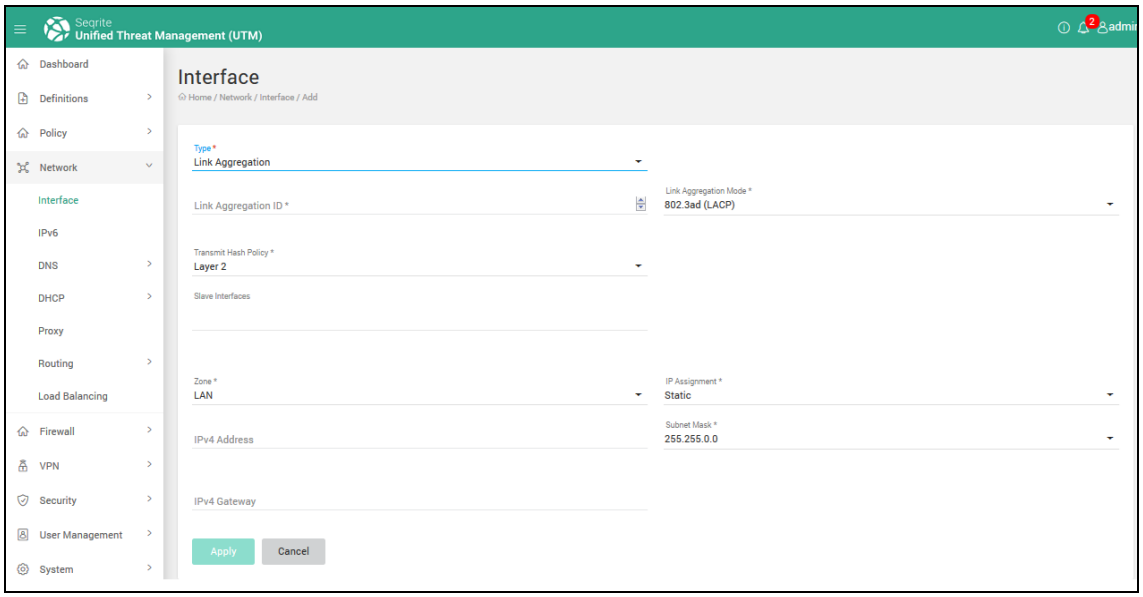
Link aggregation is a technique where multiple parallel network interfaces are combined to increase network throughput. It is used in high-speed networks to enable fast and inexpensive transmission of bulk data. Link aggregation enhances and increases the network capacity and maintains fast transmission speed without changing any hardware devices, thus reducing cost.

Link Aggregation feature offers the following two benefits:

- **Load Balancing**: The network traffic load is distributed across two or more network interfaces that appear as a single connection in order to increase reliability through redundancy.
- **Fail-over**: Combining two or more network interfaces provides fault tolerance. In case if any one of the network interfaces fail then, the traffic will be automatically directed to the other network interface.

Creating a Link Aggregation interface

1. Navigate to **Network > Interface**. The Interface page is displayed.
2. Click **Add**. The Add Interface page is displayed.



The following table explains the fields on page, configure as required:

Field	Description
Type	Select the interface type as Link aggregation from the dropdown.
Link Aggregation ID	Enter a Link Aggregation ID. This should be a unique number for identification between the range 0-99.
Link Aggregation Mode	Select the link aggregation mode. Mode specifies bonding policies that will be applied. The following modes of Link Aggregation are available: **802.3ad (LACP):** IEEE 802.3ad Dynamic link aggregation. Utilizes all slaves in the active aggregator according to the 802.3ad specification. This mode provides load balancing and fault tolerance. This mode requires a switch that supports IEEE 802.3ad LACP. **Round Robin:** This mode transmits packets in sequential order from the first available slave through the last. This mode provides load balancing and fault tolerance. **Xor:** In this mode packets are transmitted based on the transmit hash policy. This mode provides load balancing and fault tolerance. **Broadcast:** This mode transmits everything on all slave interfaces. This mode provides fault tolerance. **Active-Backup:** Only one slave in the link aggregation interface is active. A different slave becomes active if, and

Field	Description
	only if, the active slave fails. This mode provides fault tolerance.
Transmit Hash Policy	Select Transmit Hash Policy. This option will be displayed only if you select 802.3ad and Xor mode. Following are the available Transmit hash policies. **Layer 2**: Uses XOR of hardware MAC addresses to generate the hash. This algorithm will place all traffic to a particular network peer on the same slave. **Layer 2 + 3**: This policy uses a combination of layer2 and layer3 (MAC and IP address) protocol information to generate the hash. This algorithm will place all traffic to a particular network peer on the same slave.
Slave interfaces	Slave interfaces are the unconfigured physical ports that will be aggregated/merged. At least 2 and at most 8 physical ports can be aggregated in one link aggregation interface. Once configured the slave interfaces from a link aggregation interfaces cannot be removed until the link aggregation interface is deleted. These interfaces should not have VLAN interface configured on them.
Zone	Select zone. Zone can be LAN/WAN/DMZ.
IP assignment	Select IP assignment. IP assignment type can be Static or DHCP.
IPv4 address	Enter IP address.
Subnet Mask	Enter Subnet Mask. This is required only if IP is given.
IPv4 Gateway	Enter Gateway. This is required only if IP is given and zone is WAN.

3. Click **Apply**.

Note:

- VLAN and alias can be configured on Link Aggregation interface.
- Bridge cannot be configured on link aggregation interface.

Configuration at switch is required for link aggregation to work except for Active-backup mode.

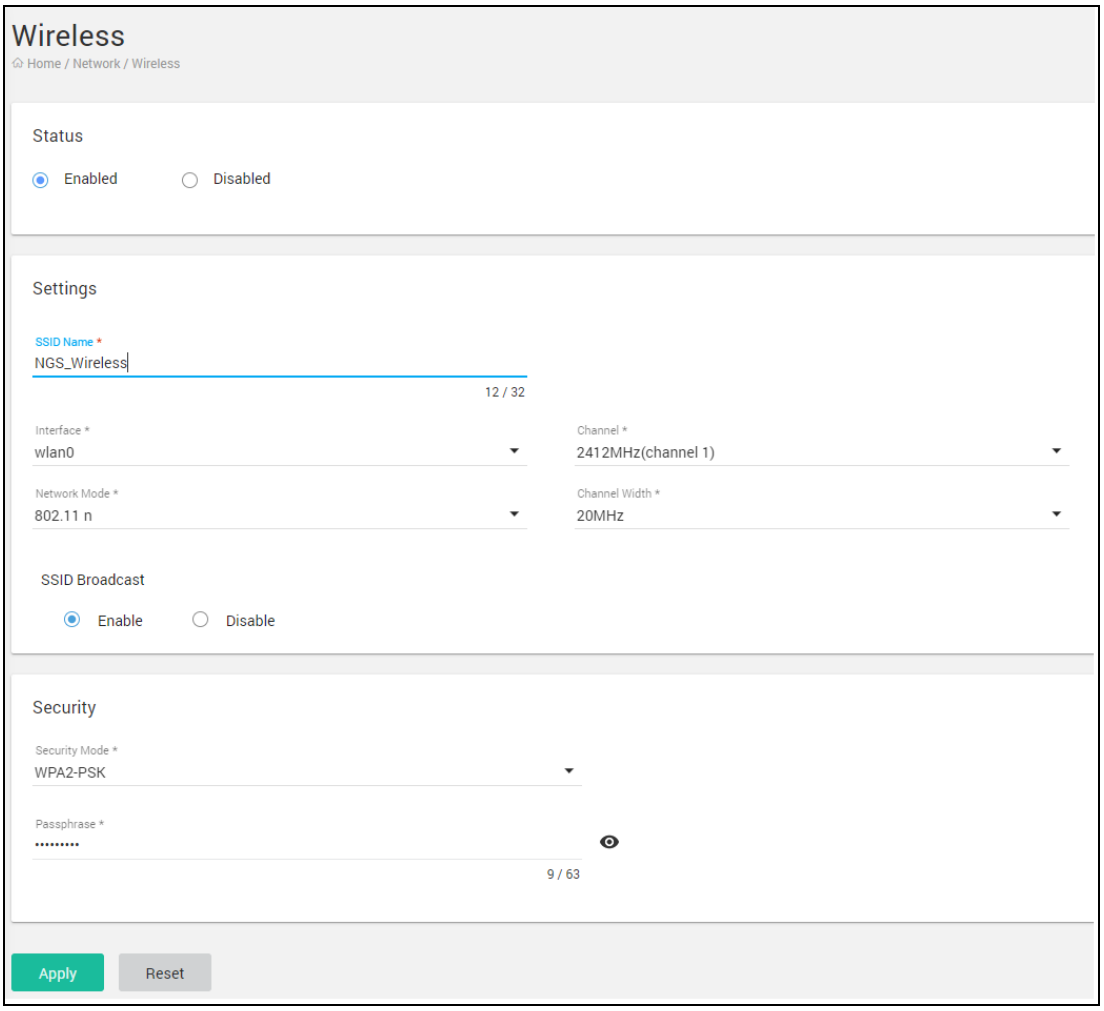
Configuring the wireless router

The NGS130W model comes with an inbuilt wireless interface. Wireless clients can connect to the UTM's wireless interface and will be treated just like the LAN users. The wireless interface is single radio broadcasting in 2.4GHz. This router supports the 802.11 b, g, and n modes. Encryption is available in WPA-PSK and WPA-PSK/WPA2-PSK modes.

Note: This feature is applicable only to the NGS130W model. The configuration page for this feature appears only if your UTM hardware device NGS130W. By default, this interface is disabled. In order for users to connect to the interface, the following configurations need to be carried out:

- Configure IP address on the "wlan0" interface in the Network > Interface page
- Configure DHCP server for wlan interface
- Configure SSID and set the security setting as per the requirement.

1. Navigate to **Network > Wireless**.



2. Select and enable the feature on your appliance.
3. In the settings area, enter the SSID for the wireless network.
4. Select the interface, channel, network mode and channel width as required.
5. Enable the SSID broadcast mode if required. If you disable the broadcast mode, the SSID will not be visible to users.
6. In the Security area, select the security mode as required and the associated passphrase.
7. Click **Apply**.

Chapter 8

Firewall

Firewall

Firewall is a network security system that helps in filtering the incoming and outgoing network traffic based on the applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted. All packets entering or leaving the intranet pass through the firewall, which examines each packet and takes specific actions on those that do not meet the specified security criteria.

Using the Firewall feature, you can set the Seqrite UTM to filter the information coming in and going out of your private network. The Seqrite UTM firewall examines each network packet. It then determines whether to forward it to the destination. As the Firewall works on the base rule *"deny everything, then allow only what is needed*", no incoming request can directly reach the private network resource. Seqrite UTM firewall allows you to create rules based on zones, service, source and, destination address. A zone is a logical group of network interfaces to which a security policy can be applied. In every rule, access is accepted/rejected/dropped based on the configured action.

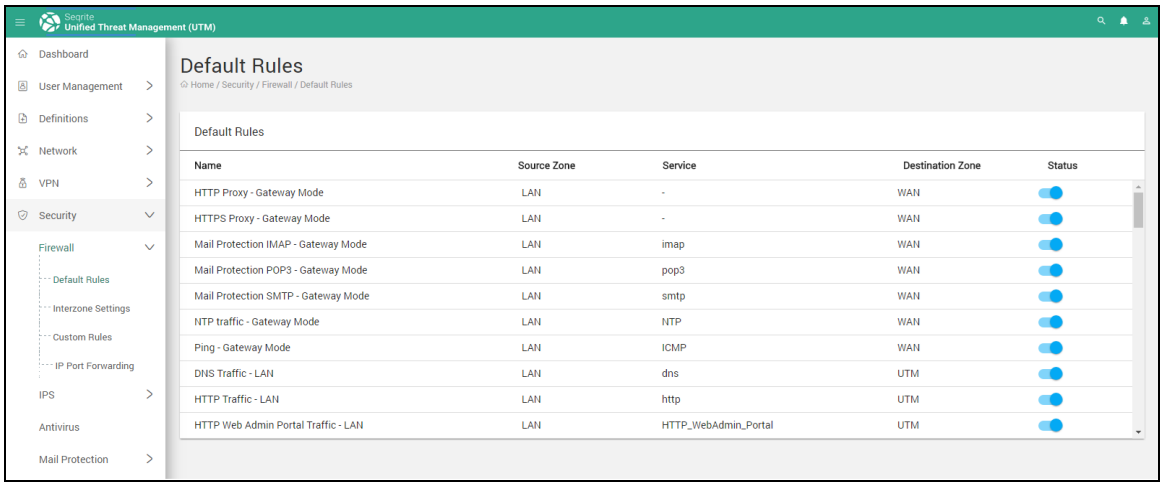
Default Firewall rules

There are few rules that need to be set by-default for some zones in firewall. These default rules are in-built on the Seqrite UTM. The Default Rules page displays the list of default rules that are set on the Seqrite UTM.

Note: The Default rules have highest priority followed by Custom rules and then the Interzone rules.

Viewing default firewall rules

1. Navigate to **Firewall > Default Rules**. The following page is displayed.



The table displays the name, source zone, service name, destination zone and status of the default firewall rules.

2. You can enable / disable the default rule using the **Status** button in the table.
3. You can search the Default rules by name using the search textbox.
4. Click on **Live Connection** to view the list of established connections through Seqrite UTM.
5. You can apply filters on connections by protocol or destination port or both. You can also search connections with source/destination IP address. To drop a connection, select and click **Drop.**

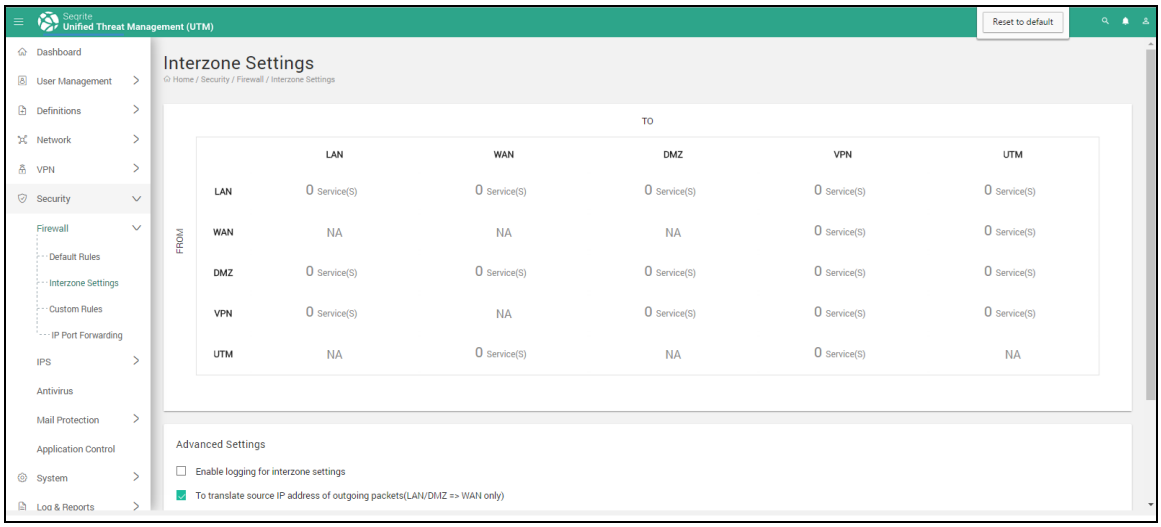
Inter-zone Rules

The Inter-zone settings page helps you to configure well known global firewall policies with a single click. This page displays a matrix which shows global inter-zone configuration for firewall setting. The rows represent the source zone and the column represents the destination zone. There are 5 predefined zones viz. LAN, WAN, DMZ, VPN and UTM. The intersecting cells show the number of services that are allowed between each source-destination zone pair. You can also edit the services under a particular combination of zones by clicking on the respective cell.

The one-click global configuration on the Inter-zone settings page allows you to configure well known services easily.

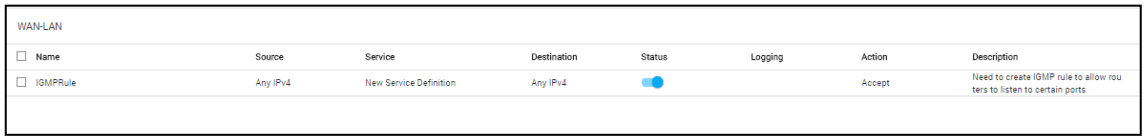
Configuring global firewall rules

1. Navigate to **Firewall > Interzone Rules**. The following page is displayed.



2. Click on the **cell** in the matrix of a particular source-destination zone pair, where you would like to add the services. The Service Definition popup is displayed, containing the list of Service Definitions.

3. Select the Service Definition that you want to allow for the source-destination zone pair. Click **OK**. You can also create a new service definition if required using the Create Definition option.



4. Select the **Logging** check box to enable logging of the changes to Interzone firewall rules.

5. To translate source IP address, you can select option for outgoing packets LAN/DMZ to WAN only. The following two options are available:

   - Masquerade: Masquerade dynamically translates the IP address. If this option is selected, then whatever address is on that outgoing interface will be applied to all the outgoing packets.

   - SNAT: SNAT applies static IP address to the outgoing packets. This option requires IP address of outgoing interface to be entered.

6. Click **Apply**.

Custom Firewall rules

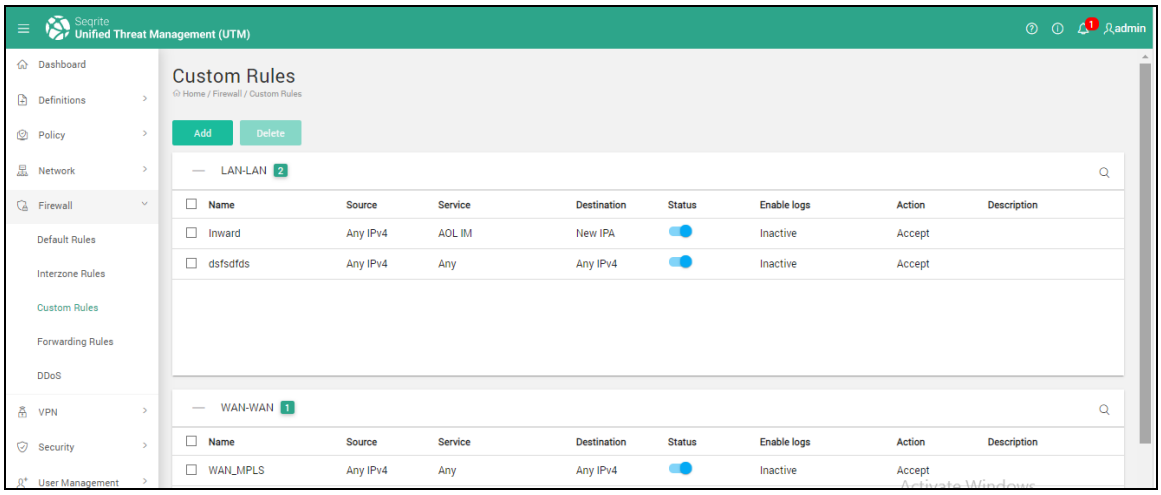
The custom firewall rules are user-defined rules that provide you with greater flexibility in defining and customizing the security policy. Using the Custom Firewall page, you can view, add, edit and delete the custom firewall rules.

Note:

If there are multiple rules for same source and destination zone, then you can change the priority of these rules. The rule that has the highest priority will be applied first.

Viewing Custom Firewall rules

1. Navigate **Firewall > Custom Rules**. The following page is displayed. The number against the group name indicates the count of rules made under that group.

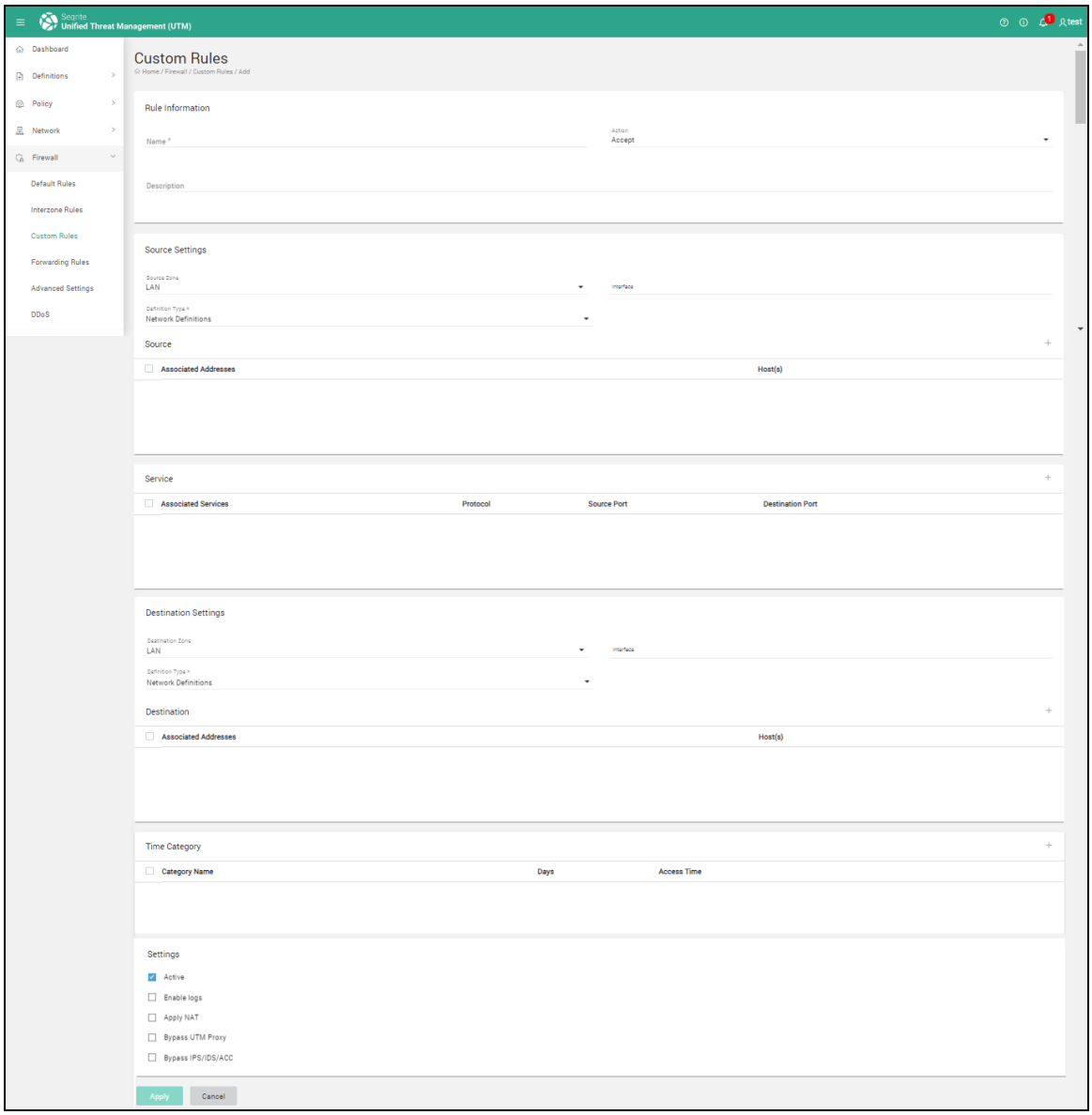


2. Click on the Group name to view firewall rules under the particular group. The Custom Firewall page displays the group-wise list of firewall rules if rules have been added.
3. Set the status of the Rule as enabled/ disabled using the button provided under the **Status** column.

Adding Firewall Rules

1. Navigate to **Firewall > Custom Rules**.
2. Click **Add**. The Add Firewall settings page will be displayed.

Firewall


Seqrite
Unified Threat Management (UTM)
test
Dashboard
Definitions
Policy
Network
Firewall
Default Rules
Interzone Rules
Custom Rules
Forwarding Rules
Advanced Settings
DDoS
Custom Rules
Home / Firewall / Custom Rules / Add
Rule Information
Name *
Action
Accept
Description
Source Settings
Source Zone
LAN
Interface
Definition Type *
Network Definitions
Source
Associated Addresses
Host(s)
Service
Associated Services
Protocol
Source Port
Destination Port
Destination Settings
Destination Zone
LAN
Interface
Definition Type *
Network Definitions
Destination
Associated Addresses
Host(s)
Time Category
Category Name
Days
Access Time
Settings
Active
Enable logs
Apply NAT
Bypass UTM Proxy
Bypass IPS/IDS/ACC
Apply
Cancel

3. The following table explains the fields on the page, configure as required.

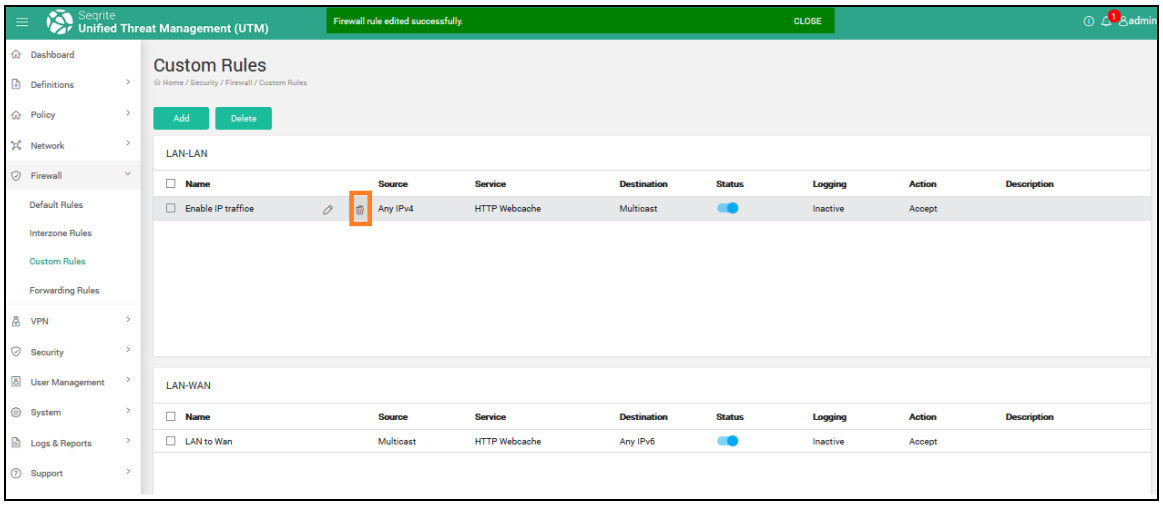
Field	Description
Name	Enter a **Name** for the rule.
Action	Select the action to be taken for the traffic as per the rule. The action can be as follows: **Accept**: Allows the connection and permits a packet to traverse through the network. **Drop**: Silently discards the packet from passing through the network and sends no response to the user. **Reject**: Rejects the connection totally and denies the packet from passing through the network. Sends an ICMP destination-unreachable response back to the source host.
Description	Enter the relevant information in this field.
Source Settings	• Select appropriate source zone from the Source Zone list. Source zone list contains LAN, WAN, DMZ, VPN, UTM and, Bridge. • Select the Source Interface. • Select the definition type, whether Network definition or FQDN definition.
Source	Select the source host or network address to which the rule will be applied. You can also add or delete the Network Definition using the respective icons.
Service	Service represents the types of Internet data transmitted via particular protocols /source ports / destination ports combination. You can browse, add or delete the Service Definitions using the respective icons.
Destination Settings	• Destination Zone Select appropriate destination zone from the Destination Zone list. Destination zone list contains LAN, WAN, DMZ, VPN, UTM and Bridge. • Destination Interface: Enter the Destination Interface. • Definition Type: Select the definition type, whether

Field	Description
	Network or FQDN.
Destination	Select the destination addresses, Use the +(Add) sign to add more destination addresses.
Time Category	Select respective time category(s), if custom firewall rule is to be effective for a specific time.
Settings	
Active	Select the status for the rule, whether Active or disabled.
Enable Logs	Select this option if you want to log activities for the firewall rule.
Apply NAT	This option is used to translate the source IP address of a host of outgoing traffic. These are of the following two types: **Masquerade**: Masquerade dynamically translates the IP address. If This option is selected, then whatever address is on that outgoing interface will be applied to all the outgoing packets. **SNAT**: SNAT applies static IP address to the outgoing packets This option requires IP address of outgoing interface to be entered.
Bypass UTM Proxy	Select this option if you want to bypass UTM web & mail proxy traffic. Policies except Internet Quota and Traffics Shaping will not be applicable to this traffic
Bypass IPS/IDS/ACC	Select this option if you want to override IPS or ACC scanning configuration. The traffic sent from mentioned host will not be scanned by IPS/ACC if enabled.

4. Click **Apply**. The rule is added and displayed in the corresponding group list.

Deleting a Firewall rule

1. Navigate to **Firewall > Custom Rules**. The following page is displayed with the list of rules in the corresponding group such as LAN-LAN or WAN - LAN:



2. Select the firewall rule that you want to delete and click the **Delete** icon (highlighted in red) as shown in the figure.
3. Click **Yes** in the confirmation box. The selected rule is deleted.

(Port) Forwarding rules

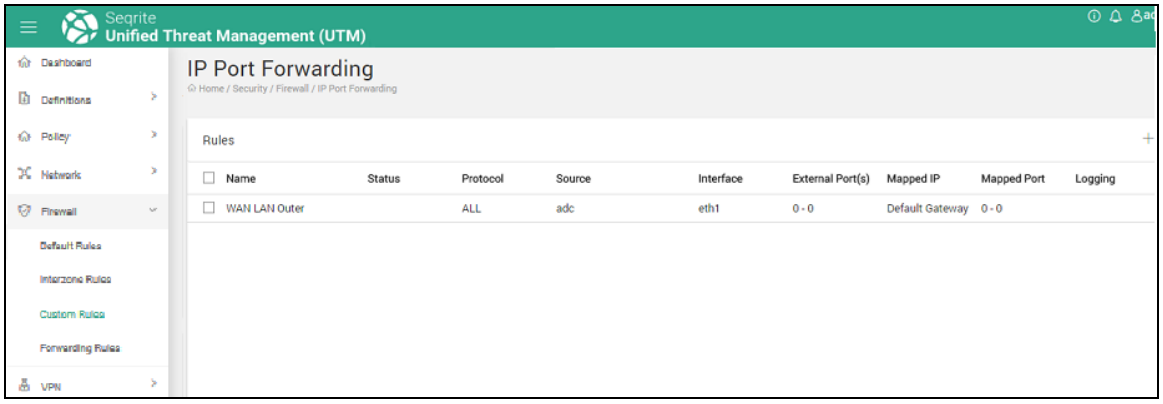
Port forwarding allows the network administrators to use one public IP address for all external communications on the Internet while dedicating multiple servers with different IP addresses and ports to the task internally. It also helps to hide from the outside world services that are running on the network.

Using the IP/Port forwarding feature on Seqrite UTM you can make a host on your network accessible to host on the Internet (outside your network), even though they are behind the Seqrite UTM. Entire IP address can be forwarded to allow access to all the ports of a computer or only specific ports can be forwarded. You can also select protocol while creating an IP/Port forwarding rule.

You can view, add, edit and delete the IP port forwarding rule using the IP port forwarding page.

Viewing IP port forwarding rule

1. Navigate to **Firewall > Forwarding Rules**. The following screen is displayed:

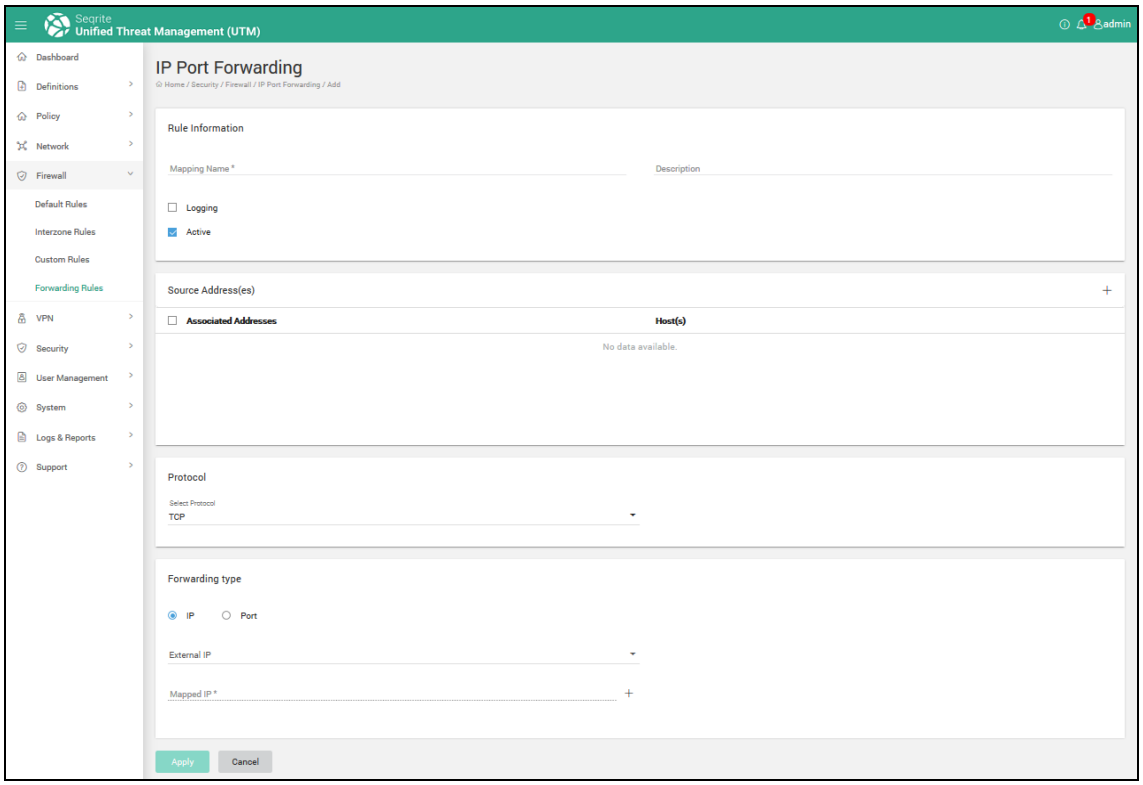


This page displays the list of IP port forwarding rules.

2. Set the status of the Rule as enabled/ disabled using the button provided under the **Status** column.
3. Select the logging option under the **Logging** column to enable logging for the rules.
4. Click **Save**.

Adding IP port forwarding rule

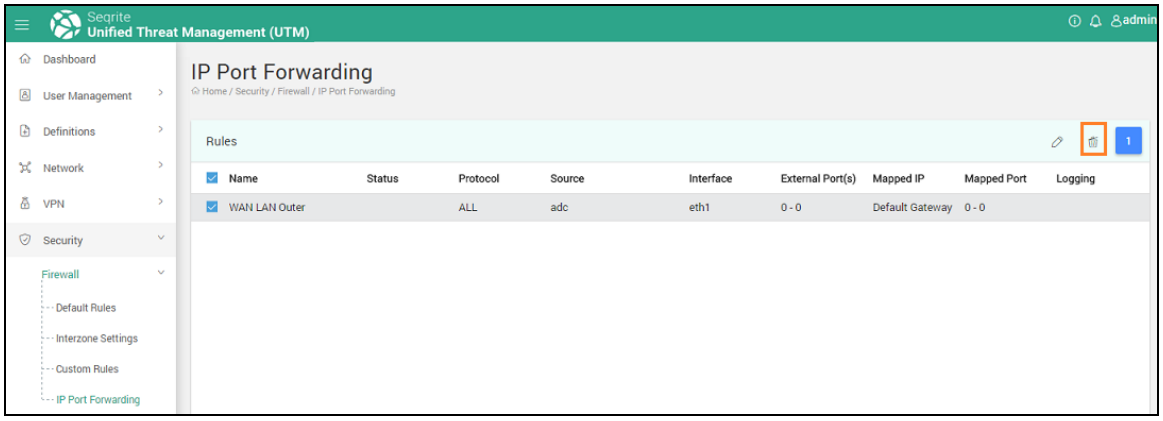
1. Navigate to **Firewall > Forwarding Rules**.
2. Click the **+ (Add)** icon. The following screen is displayed.



3. Enter the **Mapping Name** and the description for the rule.
4. Select the Enable Logs option, if you want to log the activities related to the rule. If you want to disable the port forwarding rule, remove the Active checkbox.
5. In the Source settings area, select the Definition type, whether Network or FQDN.
6. In the Source Addresses area, using the **+ (Add)** icon, browse and select from existing definitions, or use the Create Definition option to add new definitions.
7. Select a protocol from the **Select Protocol** list. Protocol list has options as ALL, TCP and UDP.
8. Select **Forwarding Type**.
   - If you select IP, you need to select external IP and browse or add mapped IP.
   - If you select Port, you need to select external IP and browse or add mapped IP along with the Port(s). You can add a range of ports as required.
9. Select **External IP.** External IP is the WAN interface IP address which will be used in forwarding. Public computers access this IP address**.**
10. Select **Mapped IP**. Mapped IP is the destination computer's IP to which the forwarding has to be done. You can browse, add or delete the IP address.
11. Click **Save**.

Deleting IP port forwarding rule

1. Navigate to **Firewall > Forwarding Rules**. The following page is displayed with the list of rules:



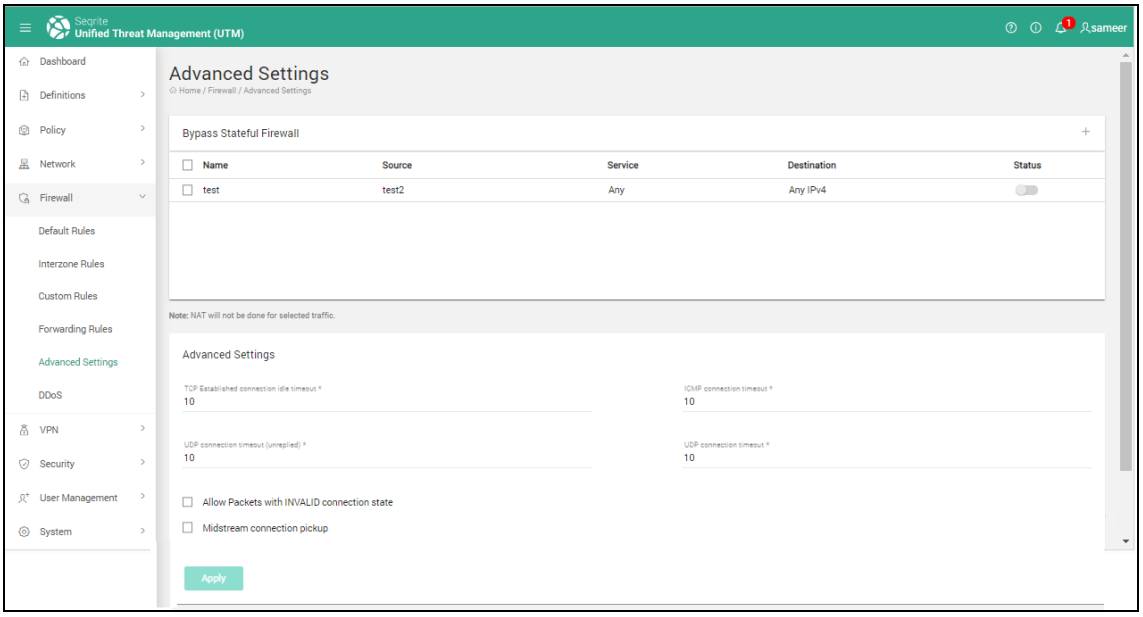
2. Select the rule that you want to delete and click the Delete icon (highlighted in red).
3. Click **Yes** on the confirmation dialog box, the IP port forwarding rule is deleted.

Advanced settings

A stateful firewall monitors the full state of active network connections and analyze traffic and data packets completely. Traffic and data packets that do not meet the set parameters are blocked. You can create rules for network traffic to bypass the Stateful firewall by configuring the source, services, and the destination and activate the rule as required.

Configuring Advanced Settings for firewall

1. Navigate to **Firewall > Advanced settings**. The page is displayed.



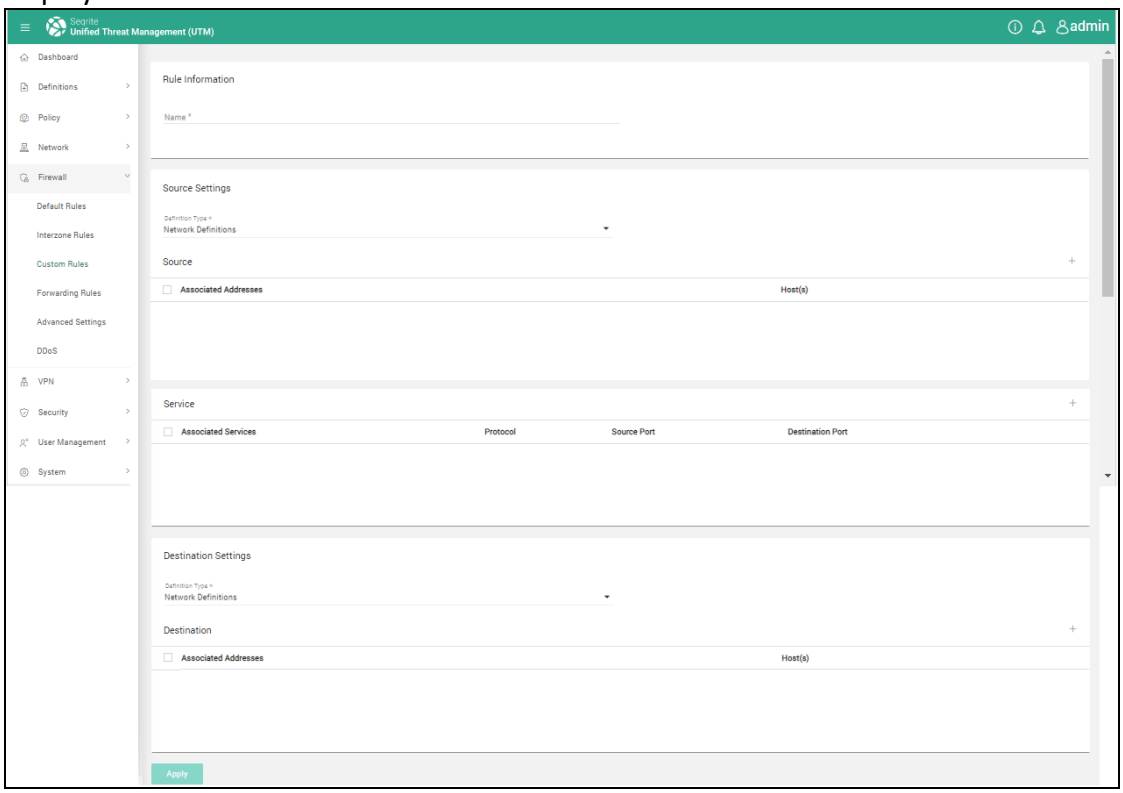
2. In the Advanced settings section, you can specify the timeout settings for TCP, ICMP, UDP connection and unreplied timeout values. You can choose to allow packets with invalid connection state and also those with midstream pickup.
3. Click **Apply**.

Creating a bypass rule

You can create a rule to bypass the Stateful firewall rules. You can then activate the rule as required.

1. Navigate to **Firewall > Advanced settings**.

2. In the Bypass Stateful firewall section, click + to create a new rule. The rule creation page is displayed.



3. Enter the rule name.
4. In the Source settings area, select the source IP address from the definitions, if not present add the required network address to definitions and select as required.
5. In the services area, click + and select the services that you want to bypass, if not present, create and then use the service definition.
6. In the destination settings area, select the destination network IP address. Add if network not present and then select.
7. Click Apply.

Distributed Denial of Service (DDoS)

A Distributed Denial of Service (DDoS) or Denial of Service (DoS) attack is a malicious attempt to make a machine, service, or network resource unavailable to its legitimate users.

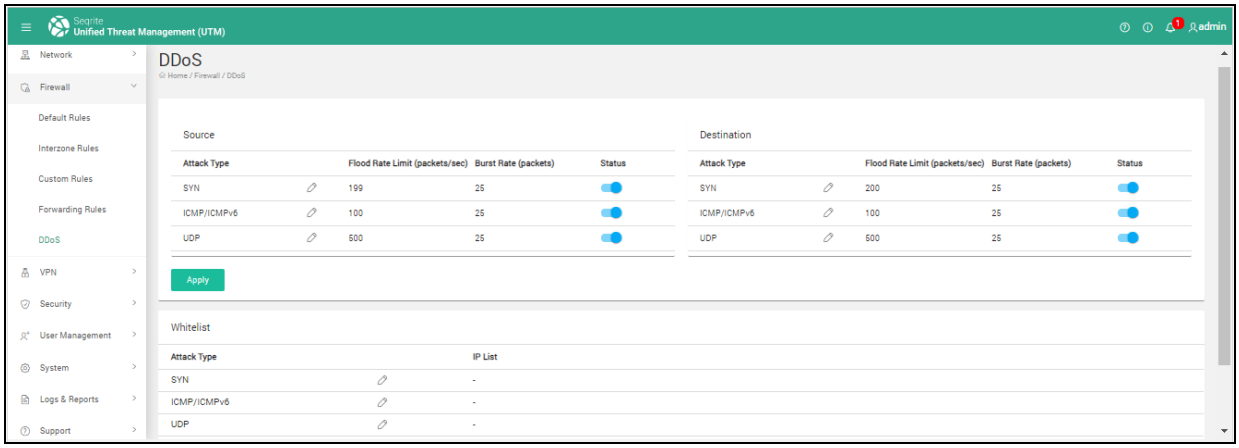
A common method of attack involves bombarding the target system with many requests, such that it cannot respond to legitimate traffic, or responds very slowly so it is essentially useless.

DoS attacks can be carried out in some of the following ways:

- SYN/TCP Flood: In this mode of attack a remote malicious host sends a flood of TCP/SYN packets, with a forged sender address. Since every packet is a connection request, the targeted resource responds with a half-open connection because it sends back a TCP/SYN-ACK packet (Acknowledge) and waits for a packet in response from the sender address (the response to the SYN-ACK packet). However, as the sender address is fake, the response never comes. These half-open connections occupy the bandwidth and the targeted resource is unable to respond to legitimate requests until after the attack ends.
- ICMP Flood: In this mode of attack, the attackers send a huge number of ICMP packets with the source address appearing as the address of the victim. The network's bandwidth is quickly used up and prevents legitimate packets from getting through to their destination.
- UDP Flood: In this mode of attack, a large number of UDP packets is sent to random ports on a remote host. For a large number of UDP packets, the victimized system will be forced into replying by sending many ICMP Destination unreachable packets, eventually leading it to be unreachable by legitimate clients.

Protecting your network from a DDoS attack

1. Navigate to **Firewall > DDoS**. The DDoS page is displayed.



2. Enable the status for SYN, ICMP, and UDP protection by toggling the corresponding status switch as required.
3. Set the Packet and the Burst rates for each of SYN, ICMP, and UDP sections in packets/sec as required.
4. Click **Apply**. After the settings are applied, UTM scans the network traffic for each of the specified protocol types. If the speed of the particular packets from a particular source exceeds the configured limit, the excessive packets are dropped and this behavior continues until the attack is over.
5. To avoid false positives of any particular type, you can add the host IP to the corresponding protocol type DDoS Whitelist. In the Whitelist section, click the edit icon next to the protocol type (SYN, ICMP & UDP type) and enter the IP address of the host and click Save. The host IP is added to the DDoS Whitelist. Packets from the configured hosts under DDoS Whitelists are treated as legitimate.

Chapter

9

VPN

Virtual private network (VPN) is a network that is constructed to connect two private networks, such as a company's internal networks over Internet for transmitting data. The systems in VPN use encryption and other security mechanisms to ensure that only authorized users can access the private network and that the data cannot be eavesdropped.

A VPN provides a secure, encrypted tunnel to transmit the data between the remote user and the company's network. The information transmitted between the two locations via the encrypted tunnel cannot be read by anyone else because the system contains several mechanisms to secure both the company's private network.

Seqrite UTM has a provision to create Virtual Private Network that allows you to securely access your organization's network over the Internet. It allows you to share keys and SSL certificates for secure authentication during connection. It also allows both site-to-site and remote connections to access the private network.

Seqrite UTM provides the following three types of VPN:

- **IPSec VPN**: This VPN uses layer 3 IP security standard to create secure tunnels between the client and the server.
- **PPTP VPN**: Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks. This VPN uses MPPE authentication for connection between client and server.
- **SSL VPN:** This VPN uses SSL certificates and Public Key Infrastructure (PKI) for authentication and encryption of the tunnel between client and server.

IPsec

Seqrite UTM allows you to configure IPSec VPN, which establishes a tunnel between a main server (For ex. Head Office) and a client server (For ex. Branch Office) and allows data to be sent through it. Both ends agree to various parameters that can be set in terms of address assignment, encryption and authentication. In IPSec a pre-shared key, RSA key or X509 Certificate is used to establish a tunnel, which helps the data to be encrypted and decrypted

and prevents snooping. This arrangement guarantees the authenticity of the sender and receiver.

There are two types of connections possible in IPSec VPN:

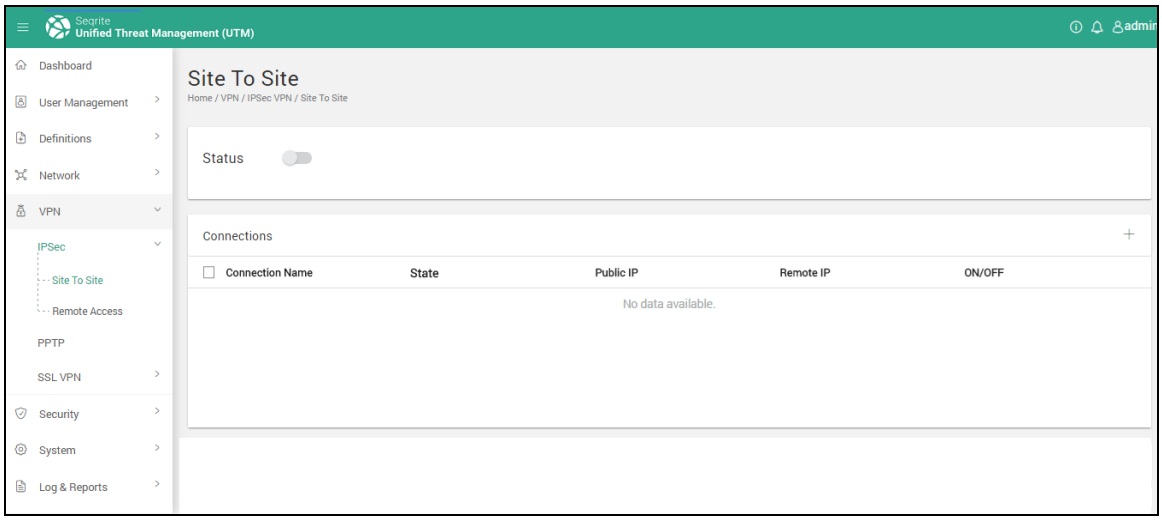
- Site-to-Site Connections – To connect the remote sites such as Head Office and Branch Office.
- Remote Access L2TP / IPSecVPN – Using L2TP (Layer Two Tunneling Protocol) to connect single VPN Client to VPN Server. Layer Two Tunneling Protocol (L2TP) is an industry standard tunneling protocol that provides encapsulation for sending Point-to-Point Protocol (PPP) frames across packet-oriented media.

Live Logs: You can also view the Live logs of IPSec VPN connections, by clicking the **Live logs** button. These logs indicate the current status of IPSec VPN service. You can export these logs to a file or select and stop a particular session using the **Stop** button.

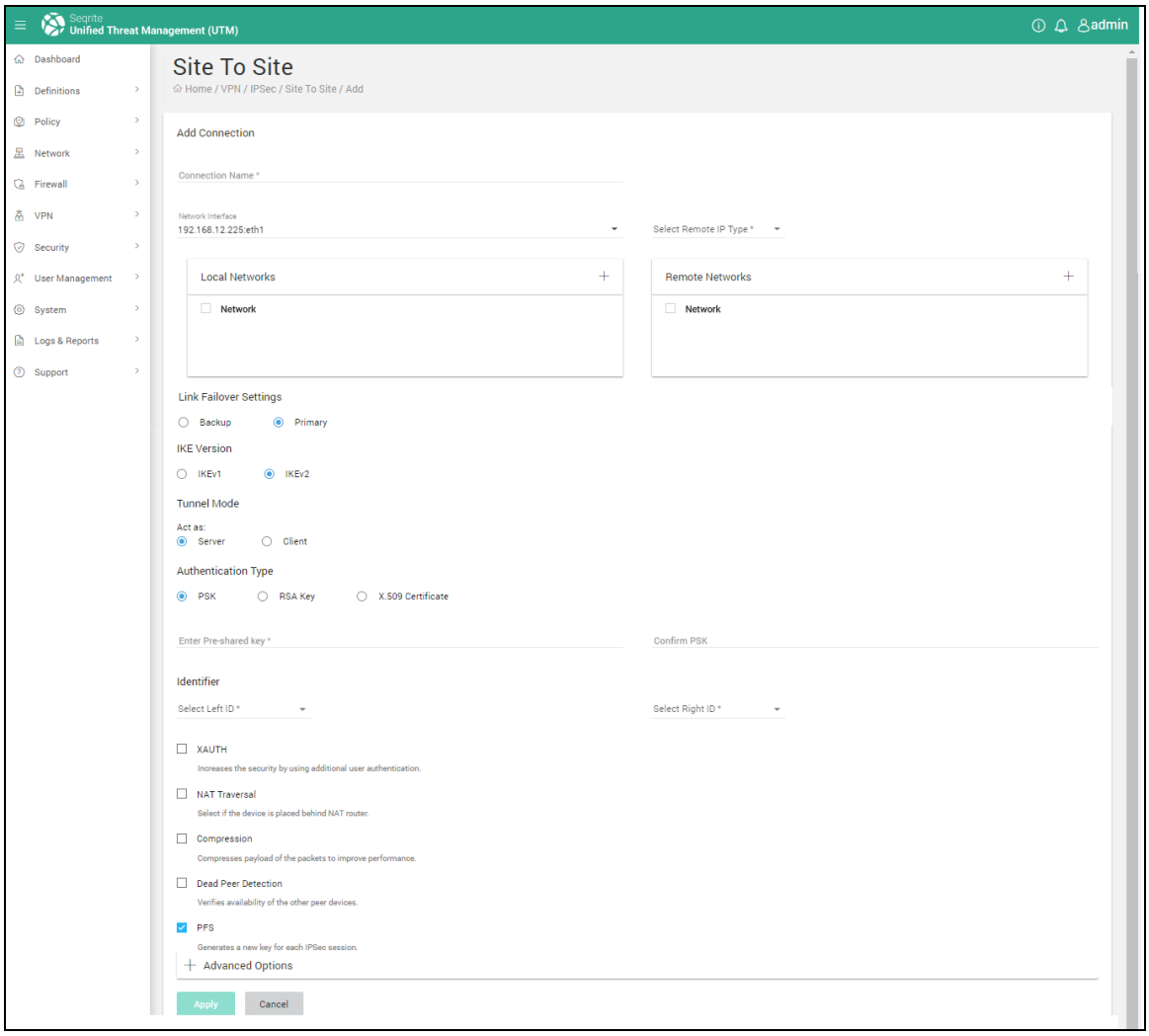
Adding an IPSec VPN Site to Site connection

Using the Site to Site IPSec VPN connection various branch networks can access the remote network such as the Head Office and Branch office.
Note: If Failover feature is configured under **Network > Load Balancing**, IPSec VPN connection also fails over to the backup interface when the primary interface/connectivity is down.

1. Navigate to **VPN > IPSec > Site to Site**. The IPSec VPN Site to Site screen is displayed with the list of VPN connections. You can also add or delete IPSec VPN connections.



2. Toggle the Status button to enable. It is disabled by default.
3. Click the + (**Add)** icon displayed on the upper right corner. The IPSec VPN Add screen is displayed.



4. The following table explains the fields on page, configure as required:

Field Name	Description
Connection Name	Enter the Connection Name. This is the unique name for the connection used for identification
Network Interface	Select the network interface on which the VPN server should be running. These are the WAN interfaces that you have configured in the Interface section.
Select Remote IP type	Click the drop-down to select the type of remote host whether **Any** or by **IP Address or Domain Name**. Enter the IP Address or Domain name if you select by IP Address or Domain Name type.
Local Networks	Select / Enter the local networks IP address and the subnet mask. You can select multiple local networks.
Remote Network	Select / Enter the Remote Network address. This are the Network

address	address of the Remote private network.
Link Failover settings	By default, primary is enabled. Use this setting to setup a backup Site-to Site IPsec VPN link for already configured VPN or MPLS link if your primary VPN fails. The list of available WAN interfaces may include your MPLS link or IPSec-Site-to-Site VPN link.
IKE version	Select the Internet Key Exchange (IKE) version. IKE is an IPsec standard protocol used to ensure security for virtual private network (VPN) negotiation and remote host or network access.
Tunnel Mode	Select whether appliance would be a server or a client to a remote host. Note: Ensure that if you select the UTM appliance to be a client, you have entered the IP address of the remote host in the by IP Address or Domain Name type under the Remote IP type selection drop-down.
Authentication Type	Select the Authentication Type from the following options: • **PSK**: The pre-shared key or PSK is a shared secret key which is shared between the two parties for using the secure network channel. You need to share this key with the remote network user. If you select this option, you need to enter a Pre shared key. • **RSA Key**: RSA is an asymmetric cryptographic algorithm used to encrypt and decrypt messages. Asymmetric means that there are two different keys out of which one is given to the Client. If you select this option, you need to share “Our Public Key” with the Client and Add the client’s public key in the “Enter Remote’s Public” text box. • **X.509 Certificate**: An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure standard to verify that a public key belongs to a user, using the identity contained within the certificate. If you select this option, you need to select the certificate, and enter the remote client’s certificate ID in the **Remote Cert’s ID** field.
Identifier	In the left side, select and enter the appropriate information for Distinct Name, Certificate ID, and FQDN of your primary UTM appliance. If you select MyIP, the default IP address of the default WAN interface is used. Enter the IP address, Distinct Name, Certificate ID and FQDN of the remote UTM appliance host on the right side. Note: You must configure exactly the opposite details on the remote host, i.e. the left side Identifier details entered on the remote UTM appliance must match with the identifier details on right for the primary UTM appliance and similarly, the right-side Identifier information for the primary UTM appliance must match the left side Identifier details of the remote UTM appliance.

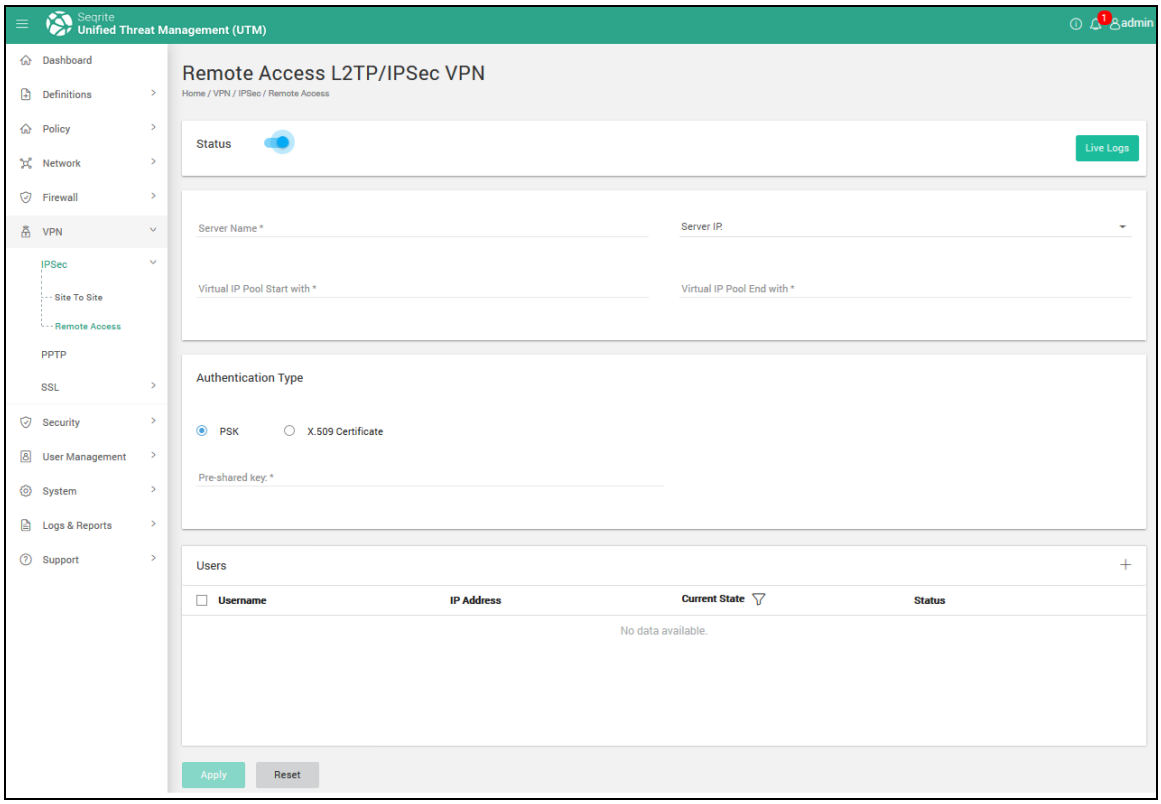
XAuth	Along with the above authorization type, you can also add extra security for authentication using the XAuth option. If you select this option, you get option for acting as a server or client, then you need to set a username and password for authentication and share this with the Client. Note: In case you have selected to Act as Client then you need to add the Username and password given by the server.
NAT Traversal	Select the NAT Traversal option if your VPN server is running on a Private IP, in order to allow the source NATed or masqueraded packets to reach the VPN server.
Compression	Select the Compression option, to compress the payload of the packets that are being exchanged on the VPN.
Dead Peer Detection	Select the Dead Peer Detection option to detect the availability of the Client / Server in the VPN. If you select this option, you need to specify the Time out period in seconds and the action to be performed to reclaim the lost resources if a peer is found inactive (dead). The following actions can be selected: Hold: Connection will be held in the same state. Clear: Removes the entire connection. Restart: Stops the current connection and reinitiates a new connection.
Advanced Options	Click the Advanced Options tab to change authentication algorithm, encryption algorithm and key group settings. Phase I allows the handshake or authentication. Phase II creates the actual tunnel. In the Advanced Options dialog box, select the Encryption Algorithm, Authentication Algorithm and the Key Group from the options available in the drop-down list. These details are used for encryption process. This setting should be the same on the Client Server.
PFS	Enabling this option generates a new key for each IPSec session.

5. Click **Apply** after entering all the required details.

Adding a Remote Access L2TP / IPSec VPN

Using the L2TP (Layer Two Tunneling Protocol) helps to connect single VPN Client to VPN Server. Layer Two Tunneling Protocol (L2TP) is an industry standard tunneling protocol that provides encapsulation for sending Point-to-Point Protocol (PPP) frames across packet-oriented media.
You can set the Pre-Shared Key and X.509 certificates for Authentication and safe access. You can set a pre shared key and then add users who can connect to the VPNs.

1. Navigate to **VPN > IPSec > Remote Access.** The following screen is displayed.



2. Toggle the **Status** button to enable. The feature is disabled by default.
3. Enter the **Server name** and **Server IP** address.
4. Enter the **Virtual IP Pool** range of IP addresses that will be assigned to the Remote users for accessing the private network.
5. Select the **Authentication Type** option from the following:
    - **PSK**: The pre-shared key or PSK is a shared secret key which is shared between the two parties for using the secure network channel. You need to share this key with the remote network user. If you select this option, you need to enter a Pre shared key.
    - **X.509 Certificate**: An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure standard to verify that a public key belongs to a user, using the identity contained within the certificate. If you select this option, you need to select the certificate.
6. In the Users section, add the details of users who are authorized to access the remote network. Click + (**Add)** icon in the **Users** section of the page. Enter the **Username**, and **password.** Confirm the password, which will be used by the users to connect to the VPN and then, click **Add**.
7. After all the details are added, click **Apply** to add Remote Access IPSec VPN.

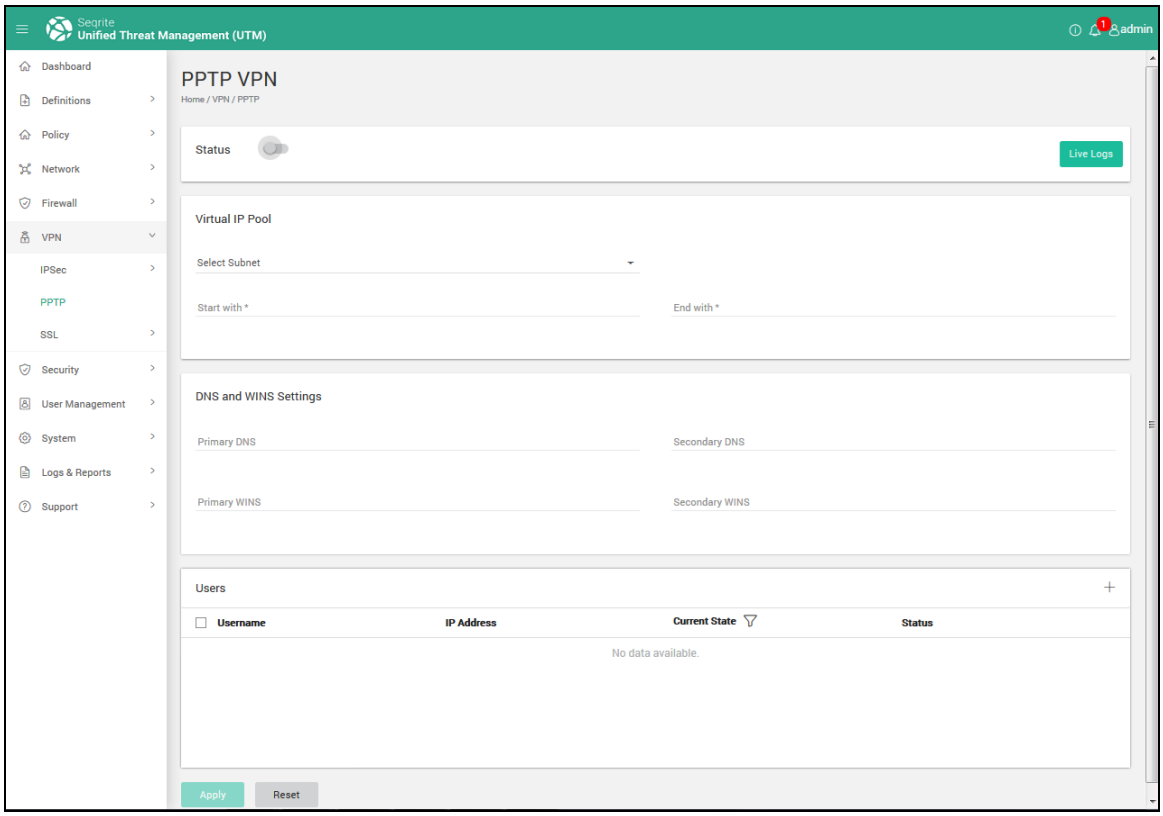
PPTP VPN

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks for Single PC access. In Seqrite UTM, the PPTP VPN allows you to connect single PC to the private network. PPTP uses plain text authentication and MPPE encryption for creating a secure tunnel for connection.

Live Logs: You can also view the Live logs of PPTP VPN connections, by clicking the Live logs button. These logs indicate the current status of PPTP VPN service.

Adding PPTP VPN

1. Navigate to **VPN > PPTP.** The following screen is displayed.



2. Select the Status as **Enabled**.
3. Enter Virtual IP pool range of the IP addresses that will be assigned to the Remote users for accessing the private network.
4. In the DNS and WINS Settings enter the IP address of the Primary / secondary DNS server and the IP address of the primary / secondary WINS server.
5. In the Users section, add the user details who can access the PPTP VPN. Click the + (Add) icon in the Users section. Enter the Username, and Password. Confirm the password required for user authentication of the user and then click **Add**.
6. After adding all the required details, click **Apply**.

SSL VPN

Secure Sockets Layer Virtual Private Network SSL VPN is a form of VPN that uses SSL certificates for authentication. It requires the installation of Road warrior client on the end user's computer. SSL VPN is used to give remote users access to web applications, client/server applications and internal network connections.

VPN

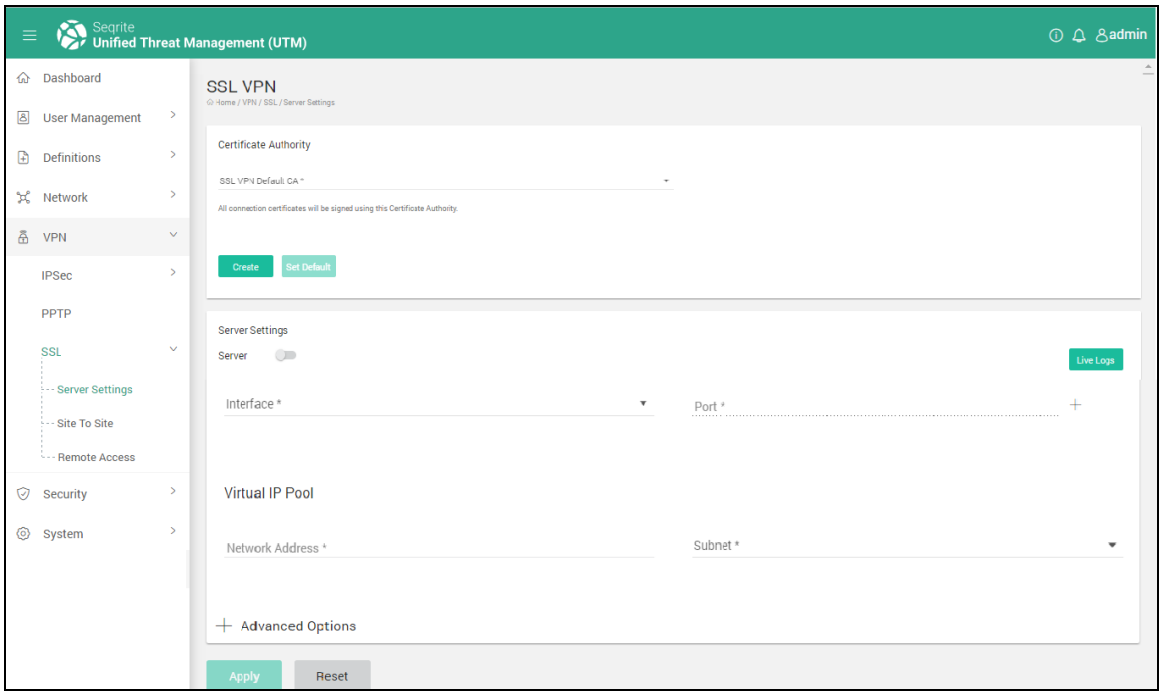
Seqrite UTM features SSL VPN that allows you to import third party certificates or create self-signed certificates. SSL VPN also provides the following types of connections:

- Server settings
- Site to Site
- Single PC remote connection

Configuring SSL VPN Server Settings

Before establishing SSL VPN connections, you need to configure the SSL VPN server on Seqrite UTM. The client will send request to this server and the server will authenticate the client as per the authentication settings. After a successful authentication the connection for communication will be established.

1. Navigate to **VPN > SSL > Server Settings**. The following screen appears.



2. Select a **Certificate Authority** for SSL VPN and set it as default using the **Set Default** button. If there is no Certificate Authority, you can also create a certificate using the **Create** button.

   Note: All the SSL VPN connection certificates will be signed by the default Certificate authority.

3. By default, the SSL VPN Server is disabled. Toggle the Server Status button to enable the server.
4. You can also view the Live logs of SSL VPN connections, by clicking the **Live logs** button. These logs indicate the current status of SSL VPN service.
5. The following table explains the fields on page, configure as required:

VPN

Field	Description
Interface	Select the Interface from the drop-down list. This is the WAN interface on which the SSL VPN will accept connections.
Port	Select only one of the ports from the following: SSLVPN-TCP: Select this protocol if remote SSL VPN server is running on TCP. Default port for TCP is 1194. Customer can add customized port for SSL VPN and configure firewall rules accordingly. SSLVPN-UDP: Select this protocol if remote SSL VPN server is running on UDP. Default port for UDP is 1194. Customer can add customized port for SSL VPN and configure firewall rules accordingly.
Virtual IP Pool	Enter the Network address of the Virtual IP Pool, these addresses will be assigned to the SSL VPN clients. Select its **Subnet**.
Advanced Options	Click on + to expand options.
Cipher	A cipher (or cypher) is an algorithm for performing encryption or decryption. Select the type of Cipher you want to use for your network from the drop-down list.
Authentication Algorithm	Select the data authentication algorithm for your network.
Diffie–Hellman Key size	The Diffie–Hellman key exchange parameter allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. You can select the length of the DH parameter.
Maximum clients	The maximum number of clients that can connect to the VPN network.
VPN Compression	Select this parameter if you want to compress the data on your SSL VPN.
Duplicate CN	Select this option if you want concurrent connections for each user.
Client to Client	Select this option to allow connectivity between any pair of

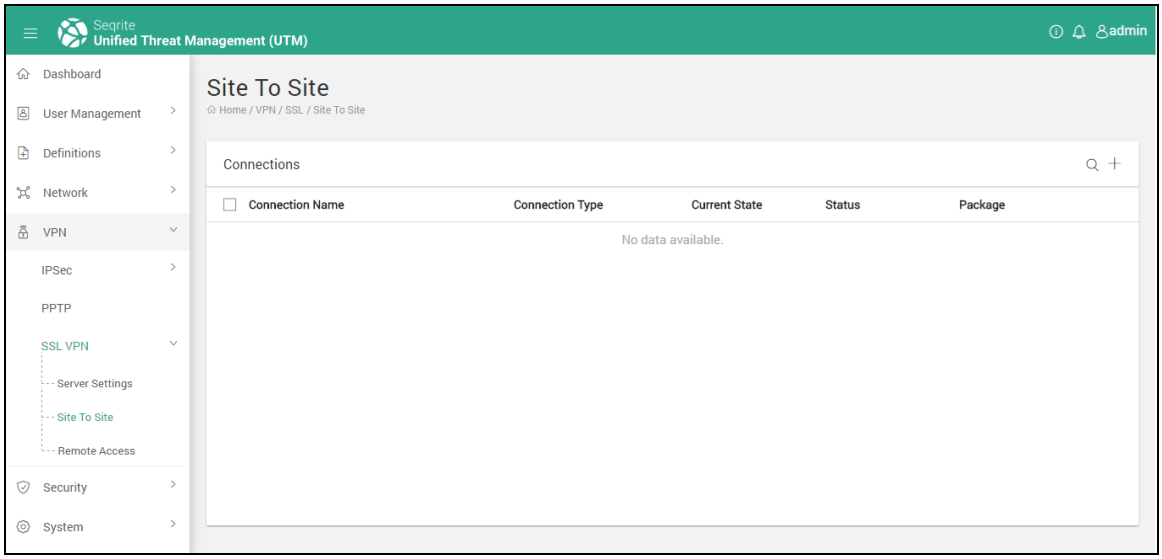
Field	Description
	remote systems.
Dead Peer Detection	Select this option if you want Seqrite UTM to detect offline remote systems.
Type of Service	Select this option to preserve the ToS bit for SSL VPN traffic.

6. After entering all required information, click **Apply** to save the changes.

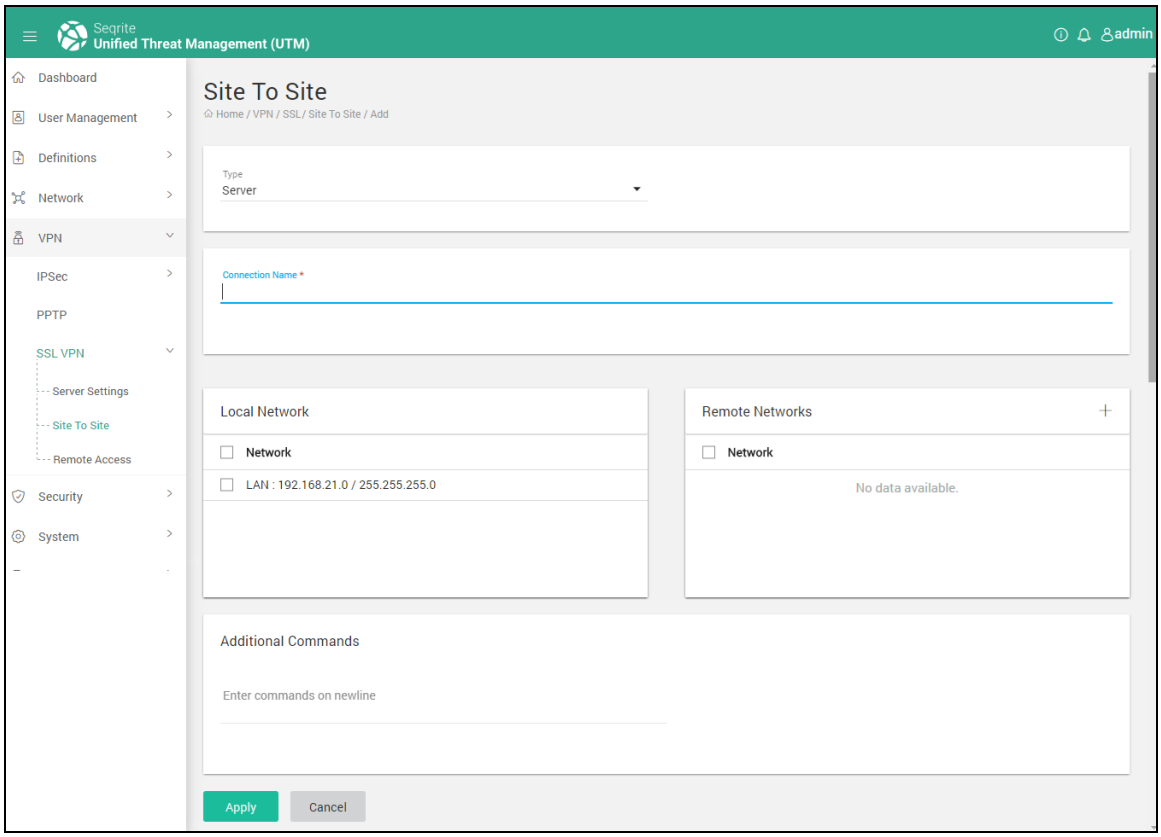
Adding site to site connections to SSL VPN

You can add sites to your VPN network so that they can have a site to site connection. You must specify the connection type whether server or client and add networks from your local networks or remote networks.

1. Navigate to **VPN > SSL > Site to Site**. The site to site configuration page is displayed.



2. Click the + (**Add)** icon on the upper right corner. The Site-to Site Add page is displayed.
3. Select the **Type** of connection you want, whether server or client.
3. If you select the Server type, the following screen is displayed:

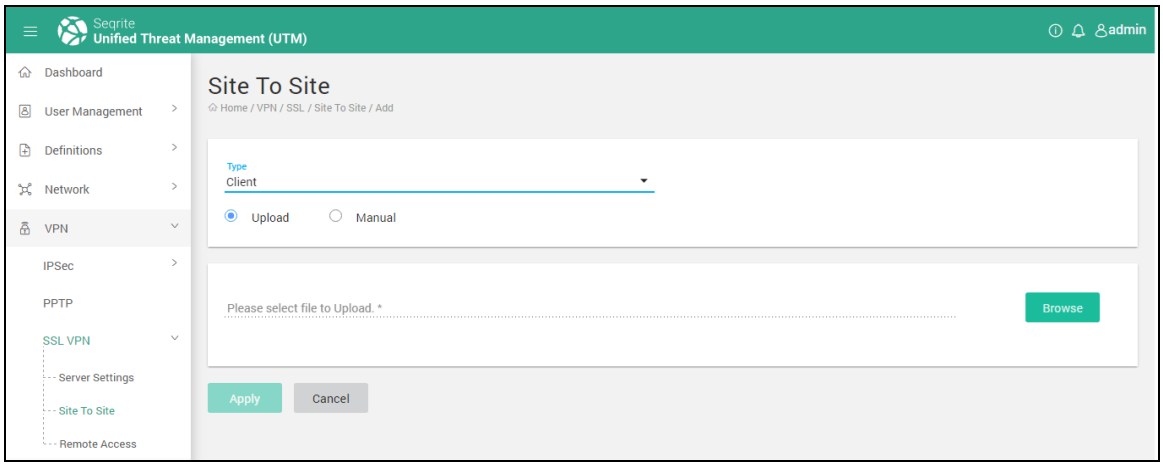


The following table explains the fields on the page, configure as required:

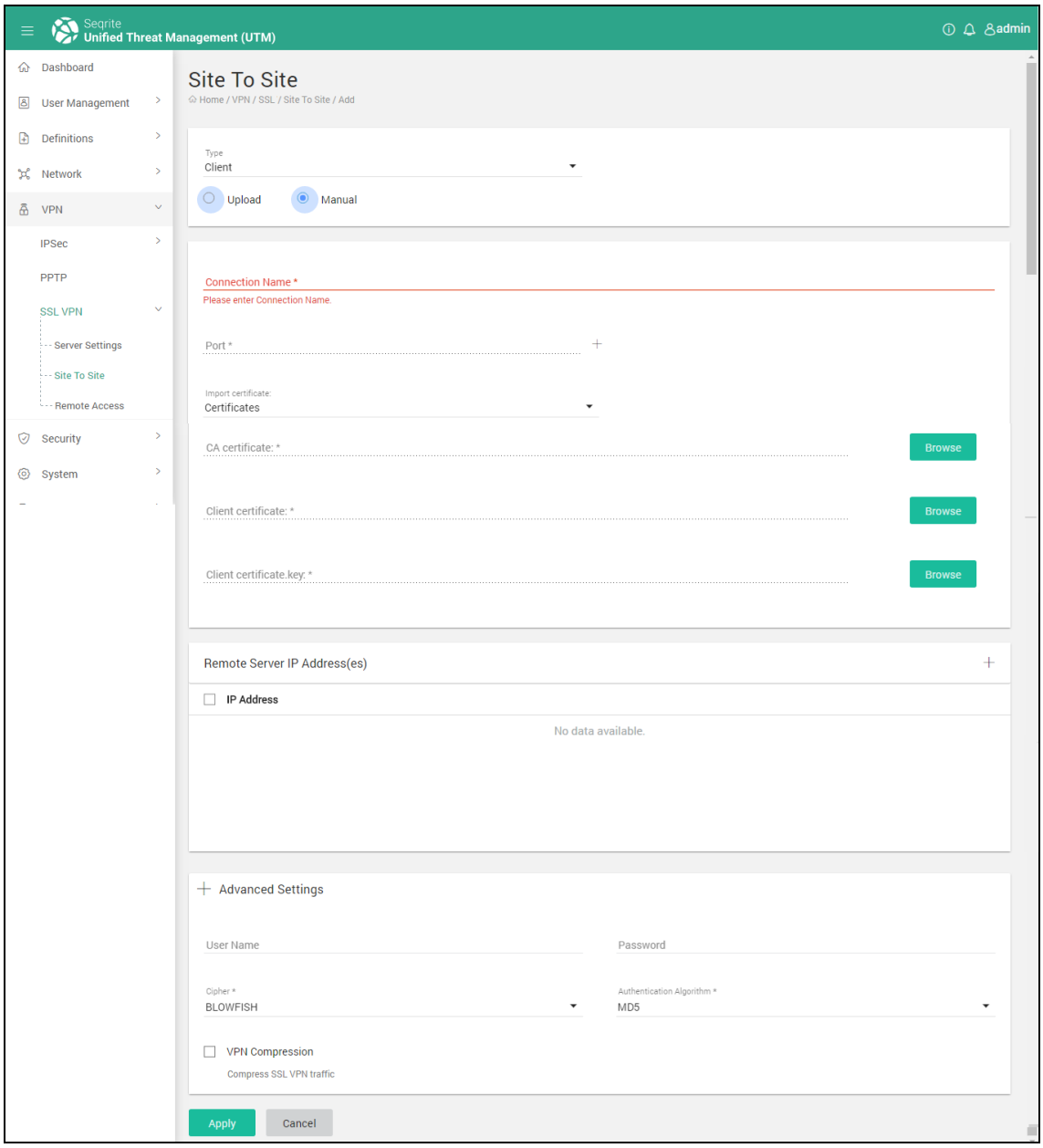
Field	Description
Connection Name	Enter a unique name for identifying the connection.
Local networks	Select the Local networks that are listed in the Local Networks section.
Remote networks	Select the Remote networks from the list displayed under the Remote Networks section. If the network that you want to add is not listed, use the **Add** button to add the network. Similarly, you can use the **Remove** button to remove the networks that you no longer need.
Additional commands	Add Additional commands if required. For example: route-gateway 10.10.16.1 ifconfig-push 10.10.16.53 255.255.255.0 redirect-gateway <def1 | local | bypass-dhcp | bypass-dns>

	dhcp-option DNS 10.10.16.100 dhcp-option WINS 10.10.16.200 route 10.10.16.0 255.255.255.0

4. If you select Connection type as **Client**, the following screen is displayed:



5. You can upload a PKG file or select to manually configure the settings. If you have the PKG file, select **Upload** option. Click **Browse** to browse and select the file.
6. If you select the **Manual** option, you must configure the following details:



The following table explains the fields, configure as required:

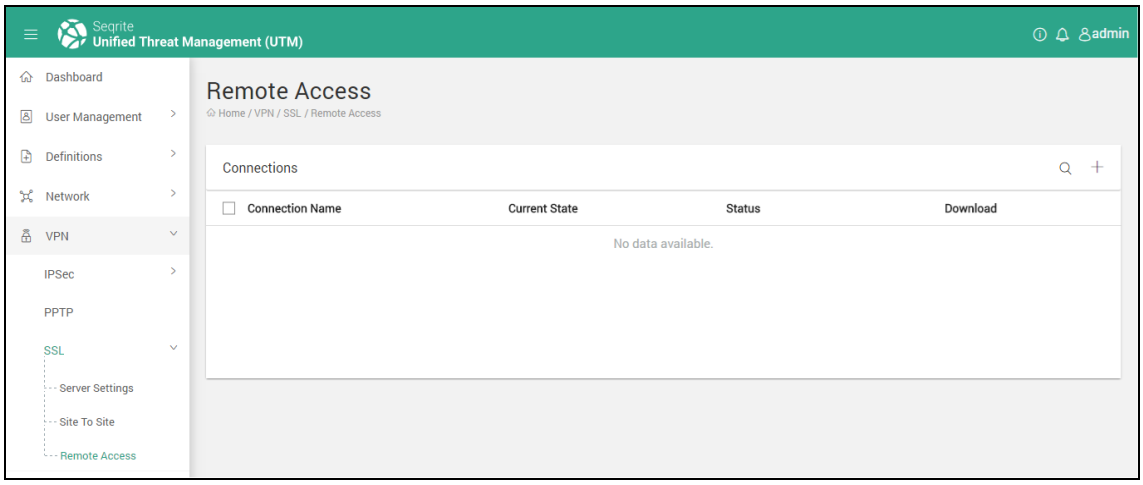
Field	Description
Connection Name	Enter the name of the connection.
Port	Add the port on which your remote SSL VPN Server is running.
Import Certificate	Certificate: You can import three files viz. CA certificate, Client certificate and Client certificate key. These files can be of .pem and .crt format. PKCS#12: Import certificate in .p12 format and provide the

Field	Description
	password for file.
Remote server IP	Enter the IP address of your remote site to which remote SSL VPN Server is bound.
Advanced Settings	Note: This setting must match on both server and client.
Username	The username provided by the third-party SSL VPN server for connection.
Password	The password provided by the third-party SSL VPN server for connection.
Cipher	A cipher (or cypher) is an algorithm for performing encryption or decryption. Select the type of Cipher you want to use for your network. This setting must match on both sides.
Authentication Algorithm	Select the data authentication algorithm for your network. Authenticate packets with given algorithm. This setting must match on both sides.
VPN Compression	Select this parameter if you want to compress the data on your SSL VPN.

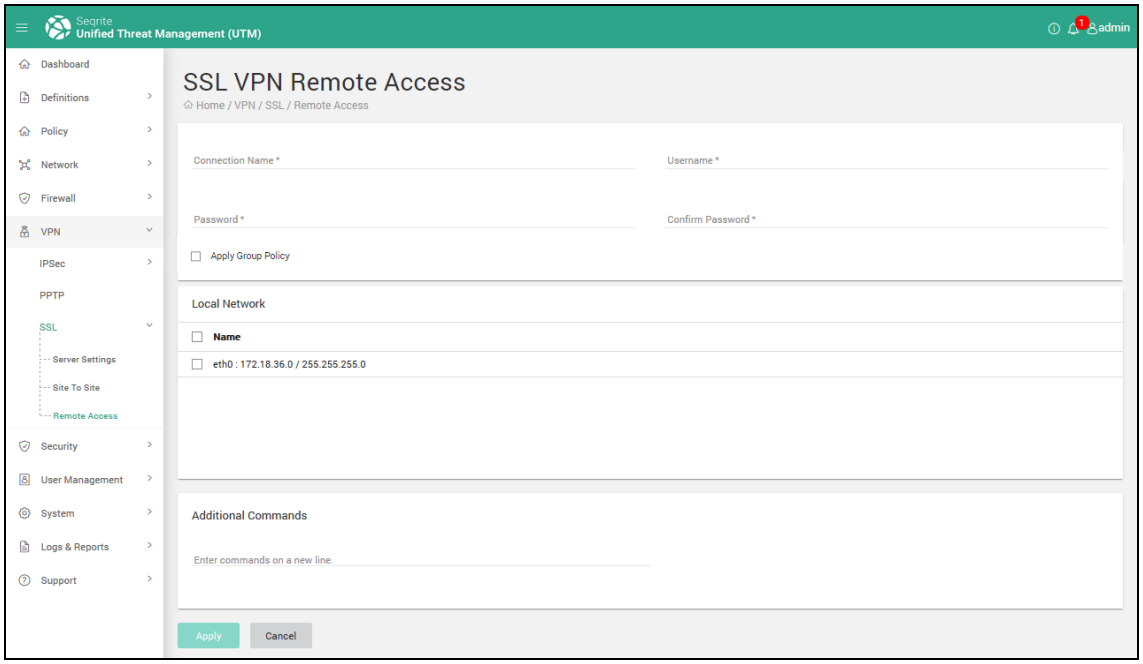
7. After entering required details, click **Apply**. After you have added the SSL Site to Site connection details, it will be displayed in the list. You can change the connection Status to ON or OFF.
8. To download a configuration package, click the **Download** link. This package is used for authentication when the Client connects to SSL VPN.

Configuring Single PC remote access for SSL VPN

1. Navigate to **VPN > SSL > Remote Access**. The SSL VPN Remote access connections list is displayed. The current connections are displayed in the list.



2. Click the **+ (Add)** icon. The Remote Access Add configuration page is displayed.



3. Enter the **Connection Name**.
4. Enter the **Username** and **Password** in the designated text boxes. Retype the Password in **Confirm Password** text box. These credentials are used for authentication. Enable the Apply Group policy check box to apply group policy settings to users connecting from outside using SSL VPN.
5. Select the **Local networks** that you want to configure for Remote Access from the networks that are listed.
6. Add **Additional Commands** if any.
7. Click **Apply**.

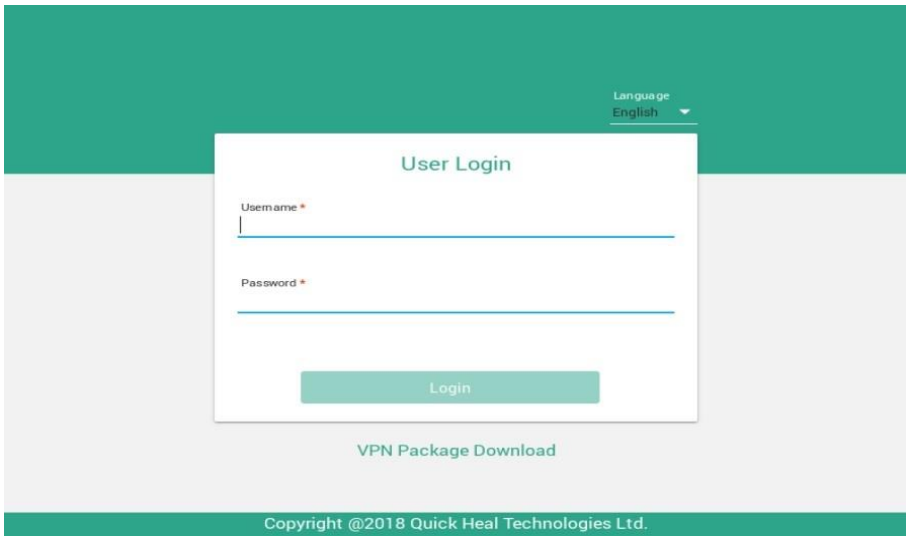
Downloading the VPN client package

If you want to access your network remotely from outside, you must install the VPN client package on your remote PC. You will also require the credentials that are set by the administrator at time of creating the SSL VPN remote user.

You can download the VPN client package for installation at the remote end in the following ways:

- Before Logging in

1. On the User login page of UTM, click VPN Package Download below the login window.



2. Enter the VPN credentials to initiate the download.

3. Select the Windows or Linux package as required.

4. Click **Submit** to initiate the download.

- After logging in
    1. Click the username in the upper right corner of the dashboard.

    2. Click on the VPN Package Download link.
    3. Enter the VPN credentials.

    4. Select the Windows or Linux package as required.
    5. Click **Submit** to initiate the download.

Chapter

10

Security

The features available under the Security menu option help you configure UTM to blocks web threats, stop malware, viruses, and phishing attacks. You can also create and enforce acceptable web usage policies.

The following Seqrite UTM features help in content filtering and protection:

- Intrusion Prevention System: Helps to protect your organization's network from external application level attacks, intrusion attempts, malwares and threats
- Antivirus: Helps in scanning the system for virus, Trojans, malwares, spywares and multiple harmful software.
- Mail Protection: Helps in scanning all the incoming and outgoing mails for viruses, threats, spams, suspicious attachments and suspicious keywords.
- Application Control: Helps in restricting insecure and low productivity applications.
- Country Based Traffic Blocking: Helps in blocking traffic to and from certain countries that are suspected to carry out cyber-attacks.

Intrusion Prevention System (IPS)

Intrusion Prevention System is a network security system that protects your organization's network from external application level attacks, intrusion attempts, malwares and threats. IPS monitors the incoming network traffic and identifies the potential threats and responds according to the rules that are set. An IPS might drop a packet that it determines to be malicious and block all further traffic from that IP address or port.

Seqrite UTM has an Intrusion Prevention System (IPS) to monitor as well as block the vulnerability exploit that attackers use to interrupt and gain control of an application or machine. The IPS has a pre-configured set of signatures embedded which are matched with the signatures of the entering data packets. If any incoming signature matches with an existing signature, the IPS either drops the packet or sets up an alarm.

The IPS can take the following actions depending on what it has been programmed to do:

- Block and drop malicious traffic from the malicious IP address.

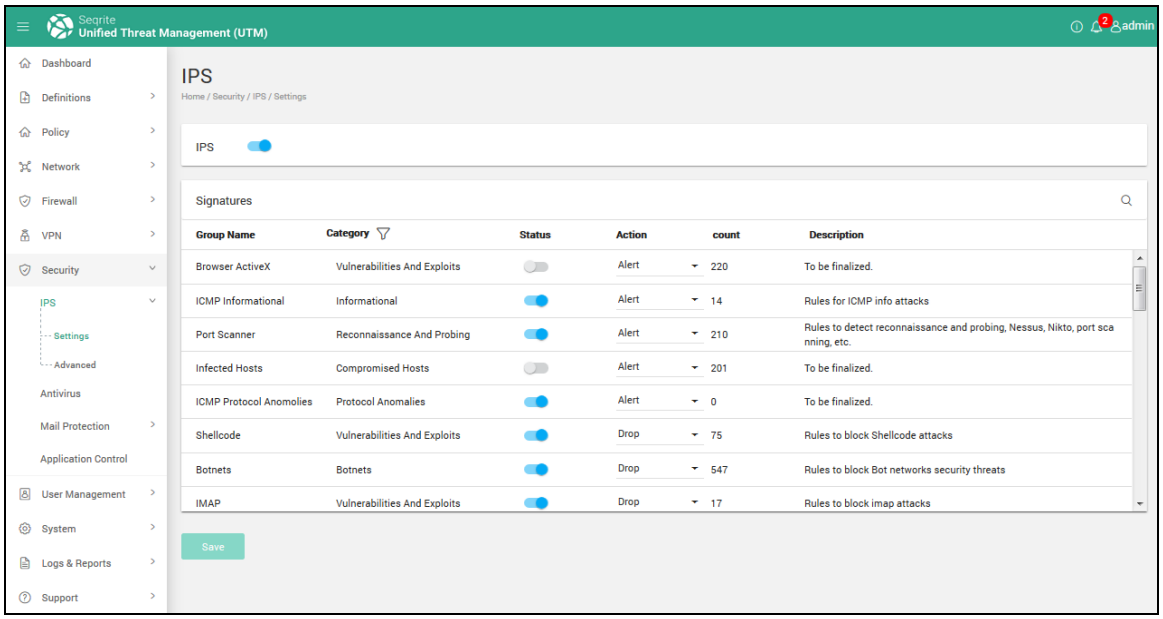
- Mark malicious IP/Network as a Black list.
- Mark good IP/Network as a White List.
- Protect your network from various types of malicious activities.

IPS Default rules and settings

This section displays the status of IPS and the various settings that fall under IPS and the relevant information such as the designated action to be taken whether to alert or drop the suspicious packet, count of occurrences, and the description.

Configuring IPS Default settings

1. Navigate to **Security > IPS > Settings**. The following page is displayed with the list of signature groups, the current status, the configured actions, the count of signatures under that category and the general description.

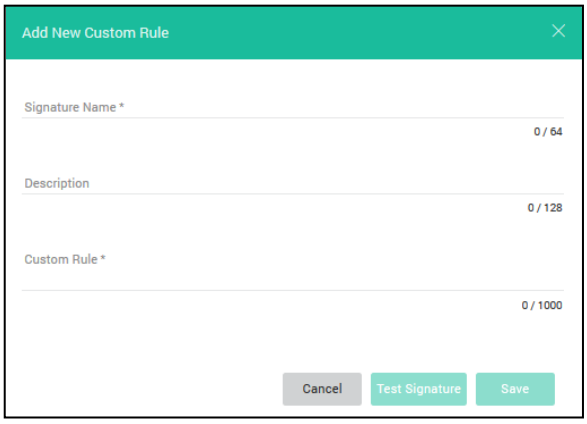


2. Configure the status and action as required for the Signature Groups that are displayed. You can set the action to the following:
   - **Alert**- The traffic continues to come into your network, but it is shown as alert under Logs and Reports.
   - **Drop**- Harmful traffic is blocked, the report is shown as blocked under Logs and Reports.
3. Click **Save** to update the setting.

Adding Custom Rules

You might need to add new signatures to your existing signature list in Seqrite UTM IPS or add your own custom signatures. You can do this using the Advanced tab on the IPS page.

1. Navigate to **Security** > **IPS**> **Advanced**. The Custom IPS screen is displayed.
2. Click **Add**. The Add New Custom rule dialog box is displayed.



3. Enter the signature name, description, and the signature in the Custom rule text box.

   Note: The name must be unique so that you know what the signature stands for. The signature must follow the format given below:

   alert/drop <Protocol> <Source IP> <Source Port> -> <Destination IP> <Destination Port> (msg:"<Message to be displayed when the signature matches>"; content:"<content to be matched in packet>"; sid:"<0 to 4294967295>")

   Note: The signature criteria can have various keyword: “value" parameters.

   The signature must be valid and must not contain any spelling or syntax mistakes.

4. Enter the custom rule.
   For e.g. alert tcp any any -> any 80 (content:"BOB"; sid:1000983;rev:1;).
5. Click **Test Signature** to test the signature. This will let you know if the signature is valid or not.
6. If the signature is validated, click **Save** to add it to the Seqrite UTM database.

White List / Black List

In Internet terminology, a white list is a generic name for a list of IP addresses that are considered harmless or genuine. Whitelists are used frequently in network security systems to allow users to compile lists of IP addresses they wish to receive or send packets to. The packets received from the addresses in this list are allowed to be delivered instead of being filtered out or blocked.

A black list contains lists of IP addresses of known vulnerability exploits, potential threats or intruders. A black list is intended to prevent intruders or suspected malicious sites from trying to communicate with your machine. The IP addresses in this list the will no longer be allowed to connect to your network. You can add or remove IP addresses to the IPS White list or Black list on Seqrite UTM.

Adding IP addresses to the White / Black list

1. Navigate to **Security > IPS > Advanced**.
2. Click **Add** in the White List section. Similarly, to add IP addresses to the Black List, click **Add** in the Black List area.
3. Add the **IP address** and select the corresponding sub-net mask of the new entry.
4. Click **Save**. The IP address is added to the respective list.

Removing IP addresses from the White / Black list

1. Navigate to **Security > IPS > Advanced**. The White list/Black List displays the IP addresses that have been added to the list.
2. Select the IP address that you want to remove from the list, click **Remove**.
3. Click Yes on the delete confirmation dialog box. The IP address will be removed from the respective list.

Enabling logs for White List/ Black List

You can enable the logs to be created for the activity related to the Black list and the White lists.

1. Navigate to **Security > IPS > Advanced**.
2. In the **Log settings** area, select the logs that you want to enable. If you want to enable logs for both Black list and White list, select both the options.

3. Click **Save**.

Configuring the traffic types for scanning

Your organization may require to monitor all inbound, outbound, as well as intranet traffic. This feature allows you to monitor all or individual traffic types. To configure different types of traffic scanning follow the steps given below:

1. Navigate to **Security > IPS > Advanced**.
2. Select Scan Request or Request and response for each incoming and outgoing type as required.
3. To disable a configured type of scan, remove the check mark against that entry. By default, the scanning for Inbound Traffic that is traffic coming from WAN is selected.
4. Enable option to scan within LAN if required.
5. Enable scanning of encrypted traffic if required.
6. Click **Save** to update the setting.

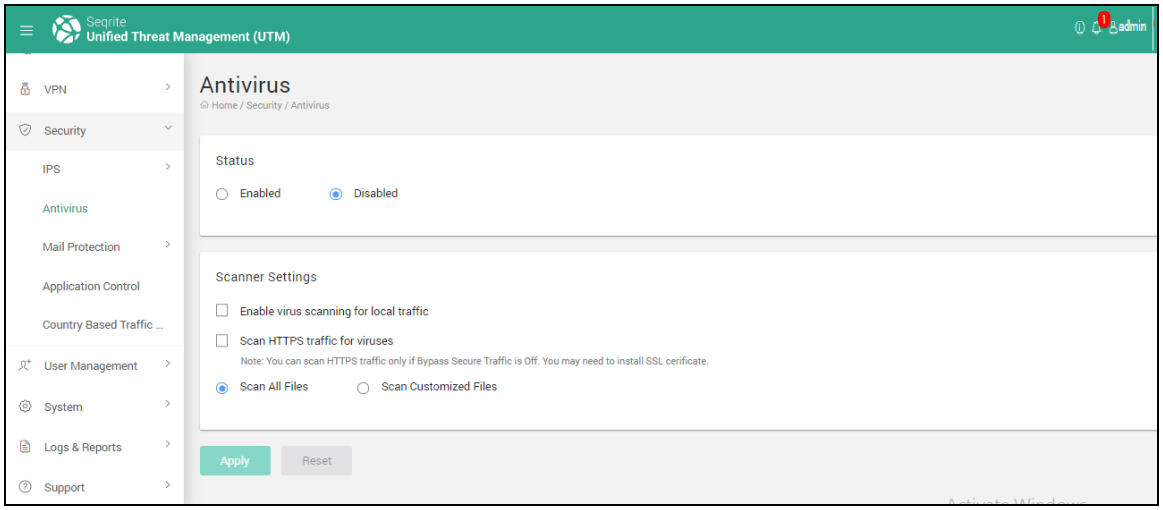
Antivirus

Antivirus software is a software used to prevent, detect and remove malicious software and infections caused by malware, including worms, Trojan horses, rootkits, spyware, keyloggers, ransomware and adware.

Using the Antivirus page, you can enable or disable the Antivirus checking on your network. You can select to scan local network and HTTPS traffic for viruses. You can specify the type of files that Seqrite UTM should scan. You can configure Seqrite UTM to report suspicious files and related statistics.

Configuring Antivirus options

1. Navigate to **Security > Antivirus**.
2. Select **Enabled** option to scan virus infections in your network.



3. In the Scanner settings option, select the **Enable virus scanning for local traffic** option if you want to enable virus scanning for Local network.
4. Use the **Scanner Settings** option to select file type for scanning. You can select all files or customized files for scanning. If you select the option as customized files, the list of file

types will be displayed. Select the required file type for scanning. You can also select to scan HTTPS traffic for virus infections.

Note: You can scan HTTPS traffic only if Bypass Secure Traffic option is Off in Internet Settings section. You may need to install SSL certificate.

5. Click **Apply**.

Mail Protection

Emails containing malicious attachment, embedded links, and malicious content are commonly used in targeted cyber intrusions. Protective policies should be imposed to ensure that the content being sent and received in an email is appropriately classified to go across the network. Enforcement of protective policies on emails helps to minimize the number of data spills and the exfiltration of data from the network via email. The Mail protection feature provides email filtration by scanning inbound and outbound emails and make configuration for the following:

- Global Settings (Mail Protection)
- Antivirus scanning
- Anti-spam scanning
- Attachment control
- Keyword based email blocking

Note: For IMAP sever only Antivirus scanning feature is available.

Logging of action and reporting from the email filter is done which can be used for auditing. Effective logging and auditing help to identify security incidents and the administrator can check the logs to know why the email was blocked and to determine if the email / content should be allowed.

Global Settings

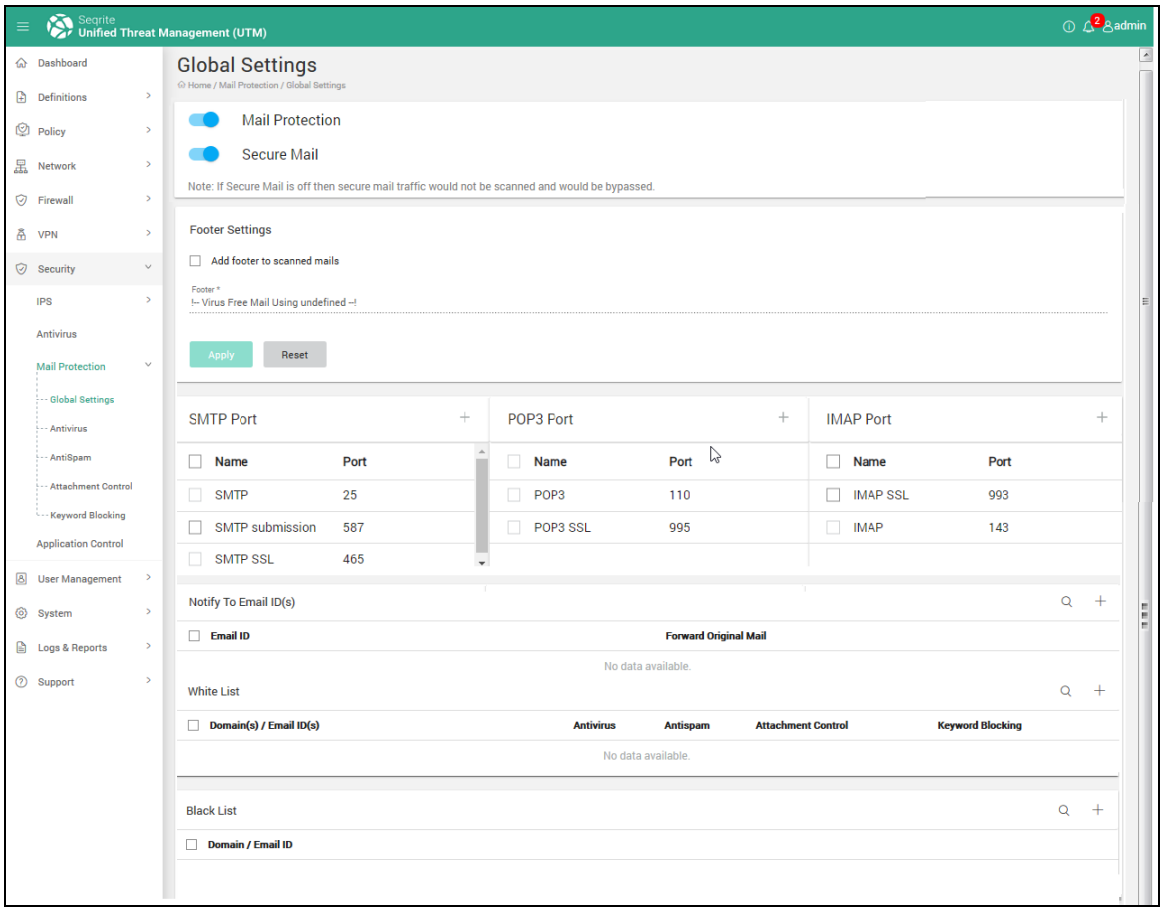
Using the global settings page, you can configure the following settings that will be applicable for all types of mail scanning:

- Select and set the footer message to append to the scanned emails
- Configure the mail server port, as the listening port of mail server SMTP, POP3, and IMAP.
- Add the email addresses to which you want to send notifications. These Notifications contain the suspicious email details and blocked emails.
- Add domains / email ids to whitelist, so that the mails coming from and going to these domains / email addresses will not be scanned for virus, spam, attachment control and keyword blocking.

- Add domains / email addresses to blacklist, in order to block emails coming from and going to these domains / email ids.

Configuring the mail protection global settings

1. Navigate to **Security > Mail Protection > Global Settings**. The following page is displayed.



2. Toggle and set the **Mail Protection** option as Enabled.
   Note: If mail protection is disabled then firewall rules for the corresponding ports should be configured.
3. Enable secure mail option if you want to scan secure SMTP and POP3 mail.
   Note: This feature will be enabled by default. You can disable it if required.
4. Enable the Footer option **Add Footer to scanned mails** if you want to append a footer message in all incoming and outgoing email message. Enter the message that you want to append in the footer of email in the given text box.
   For e.g., you can declare the email/attachment as virus-free.
   Click **Apply** to apply Footer message.
5. Enter the mail server port, for SMTP, POP3 and IMAP. Use the **+(Add)** button to browse through the definitions or to create a new definition if required.

6. In the **Notify to email IDs** section you can add email address that will receive notification about the infected and suspicious email. You can also forward the blocked / suspicious emails as attachments to these email ids. Click **+ (Add)** icon in the Notify to email IDs section. Select the option to forward the original email (that may be suspicious or infected) if required.
7. Click **Save.**

   Note: To receive an e-mail notification, you need to configure SMTP settings first.
8. To add email address to the whitelist, click the +(**Add)** icon in the whitelist section. The Whitelist popup is displayed. Select the white list type, if you want to whitelist a domain or email address. Enter the domain address / email address in the Address field. Select the modules for which you want to whitelist domain/ email address. Mails from these domains and email addresses will not be scanned.

   Note: You can apply the configured whitelist settings simultaneously to the White list for Antivirus, Antispam, Attachment control and Keyword Blocking by selecting the available options.
9. Click **Save**.

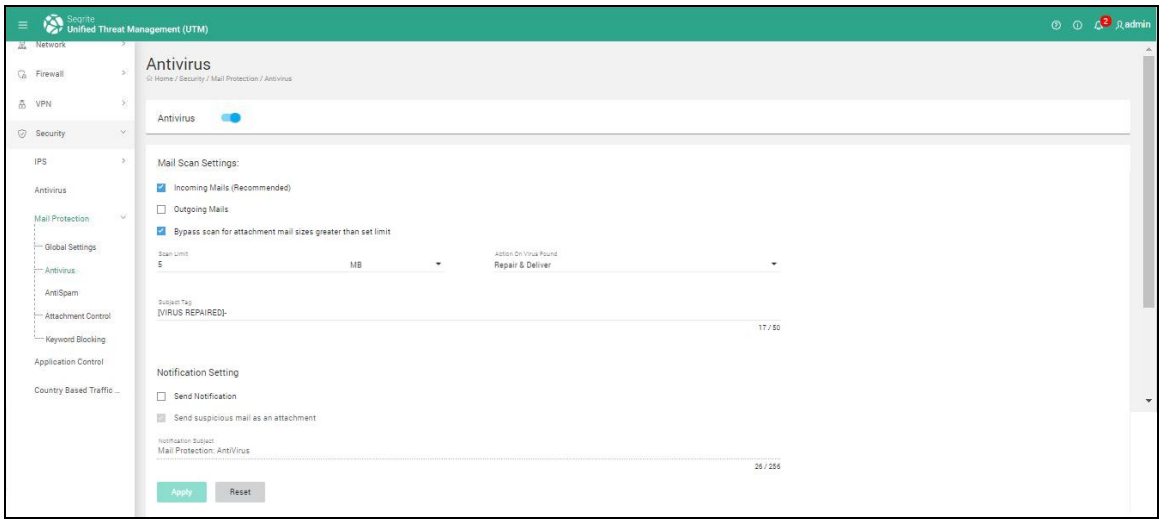
   Note: The Email address configured in SMTP settings is whitelisted by default.
10. To add Domain / email address to the blacklist, click **Add** in the blacklist section. Enter Email ID / Domain name and click **Save**. Mail from blacklisted listed domains and email addresses will be blocked.
    Note: Blacklist has a higher priority than Whitelist.

Antivirus protection for mail

The Antivirus feature allows you to scan the mails that are sent and received. You can select to scan all outgoing or incoming mail or both. You can also set a mail size to be allowed to scan, emails exceeding the size limit will not be scanned for virus. You can also configure Seqrite UTM to notify the administrator in case a virus is detected and take an action on the infected mail.

Configuring Antivirus settings for mail protection

1. Navigate to **Security > Mail Protection > Antivirus.** The following page is displayed.



2. Toggle the Antivirus scanning option to enable the feature.
3. Select the option to scan incoming or outgoing mail. By default, incoming mails are selected for scanning.
4. Enable the option to **Bypass scan for attachment mail sizes greater than set limit** if you want to skip scanning emails of large size. Enter the size limit in MB or KB. If the email size is more than the specified size it will not be scanned for virus.

   Note: The size is the MIME size of email.
5. Select the **Action on Virus Found** in the email from the drop-down list:
   - Send Original: The original email will be sent. This email may contain virus and can be harmful.
   - Repair and deliver: This option, attempts to repair the malicious email and then deliver it to the recipient. (Selected by default)
   - Delete and deliver: This option deletes the infected attachment of the email and delivers the email.
   - Do not deliver: The infected email will be blocked.
6. Select the option to add a **Subject Tag** to the scanned emails. Enter the subject tag you would like to append to the email in the given textbox.
7. In the Notification Setting area, select the **Send Notification** option to send a notification to the administrator about the infected emails. Enter the subject tag for the notification email. You can also select the option to attach the infected / suspicious email and send it to the administrator.
8. Click **Apply**.

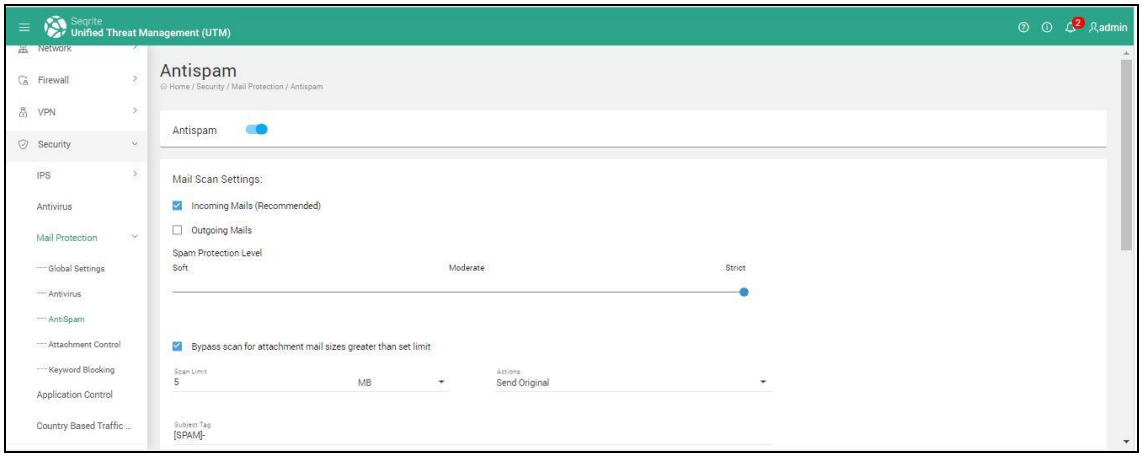
AntiSpam

Email spam also known as unsolicited bulk E-mail (UBE), junk mail, or unsolicited commercial e-mail (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. An anti-spam feature helps to prevent email spam or unsolicited bulk emails from entering email systems using various techniques.

The Seqrite UTM Antispam feature helps you to scan the emails and check for spams. Anti-spam, when enabled, helps you set a spam protection level which helps in considering emails as Spam.

Configuring AntiSpam settings

1. Navigate to **Security > Mail Protection > AntiSpam**. The following screen is displayed.



2. Toggle the status switch to enable the feature to scan all the incoming mails for spam.
3. In the Scan mail section, select the option whether to scan only incoming mail or both incoming and outgoing mail for spam.
4. Use the **Spam protection Level** slider to set a required level of protection. By default, the spam protection level is set to moderate that you can change as required. The following options are available:
   - Soft: Indicates the emails are normal with less criticality.
   - Moderate: Indicates the emails are critical and of moderate level. A good number of emails will be tagged as Spam.
   - Strict: Indicates the emails are critical and of high level. A large number of emails will be tagged as Spam
5. Select the option for **Bypass scan for attachment mail size greater than set limit** and specify the size of the email in MB or KB. If the emails size is more than the specified size, then it will not be scanned for spam.

Note: The size is the MIME size of email.

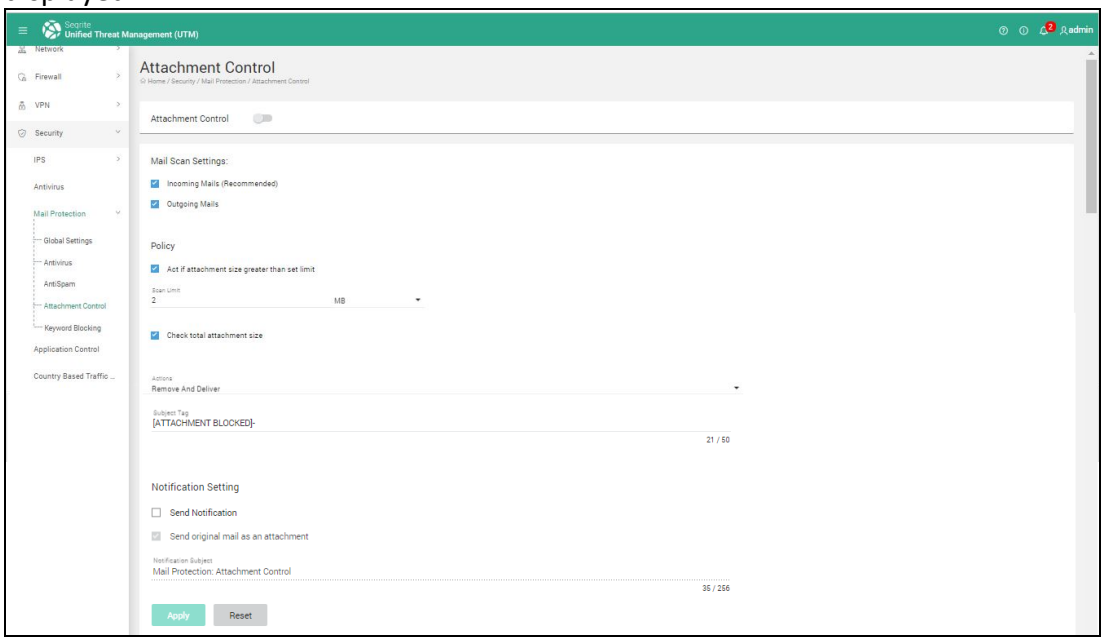
6. Select **Action** to be taken on the spam email from the following two actions:
    - Send original: Sends the original email to the recipients.
    - Do not deliver: The Spam email will be blocked.
7. Select the **Subject Tag** option if you want to prefix to the email subject if spam email is detected. Enter the Subject Tag in the given textbox.
8. Select the **Send Notification** option to send a notification to the administrator about the spam emails. Enter the subject tag for the notification email. You can also select the option to attach the suspicious email and send it to the Admin. Click **Apply** to save and apply the settings.
9. Use the **+ (Add)** icon to add email addresses and domains to Spam blacklist. A Spam blacklist contains the email addresses/domains whose mails have to be scanned irrespective of their contents. Thus, mails from the addresses/domains listed here will be tagged as "SPAM". This feature will be specifically evoked in case some server has an Open Relay which is being misused by Mass Mailers and viruses.
10. Click **Save**.
11. To save the configurations on Antispam page, click **Apply**.

Attachment Control

Attachment control feature helps you to scan the files that can be attached and sent or received in an email. You can specify the limit of the attachment size. If the attachment is greater than the specified size, then the set actions will be taken. This applies for both incoming and outgoing mails. You can also specify the extension type and the content type for the attachments that can be allowed or blocked. The content of the file helps to determine the file type. The file extensions can be changed and therefore a mismatch between a file's type and its extension can be treated as suspicious and blocked.

Configuring attachment control

1. Navigate to **Security > Mail Protection > Attachment Control**. The following screen is displayed.



2. Select the Attachment Control status as **Enabled**.
3. Configure the **Scan Mail** options. You can set whether to scan only incoming mails or both incoming and outgoing mails for attachment control.
4. In the Policy section, select the option **Act if attachment size greater than set limit** to scan email with the specified attachment size and specify the size. Emails containing attachment greater than the specified size will be scanned. You can also select to add up the total size of the attachments in the email. For example, if there are 3 files attached to the email of 2 MB each. Then the total attachment size will be 6 MB.

   Note: The size is the MIME size of email.
5. Select **Action** to be taken on the spam email from the following two actions:
   - Send original: Sends the original email.
   - Remove and Deliver: Removes the attachment and sends the email. Enter the subject tag to be appended to mail: For e.g.: Attachment Blocked.
   - Do not deliver: For SMTP email will be blocked, for POP3 original mail without attachment will be sent.
6. In the Notification Settings section, enable the option to send notifications to the administrator about the malicious attachment in the emails. The option to attach the suspicious email and send it to the Admin is enabled by default. Enter the subject tag for the notification email.

7. In the File Types section select the file types for attachments that you want to block. Add, browse the file type using the icons provided. The file type contains extension and content type.
   Note: Deleting the file type will only remove the file type from the list.
8. Click **Apply** to save the configurations**.** Click **Reset** if you want to configure the options again.

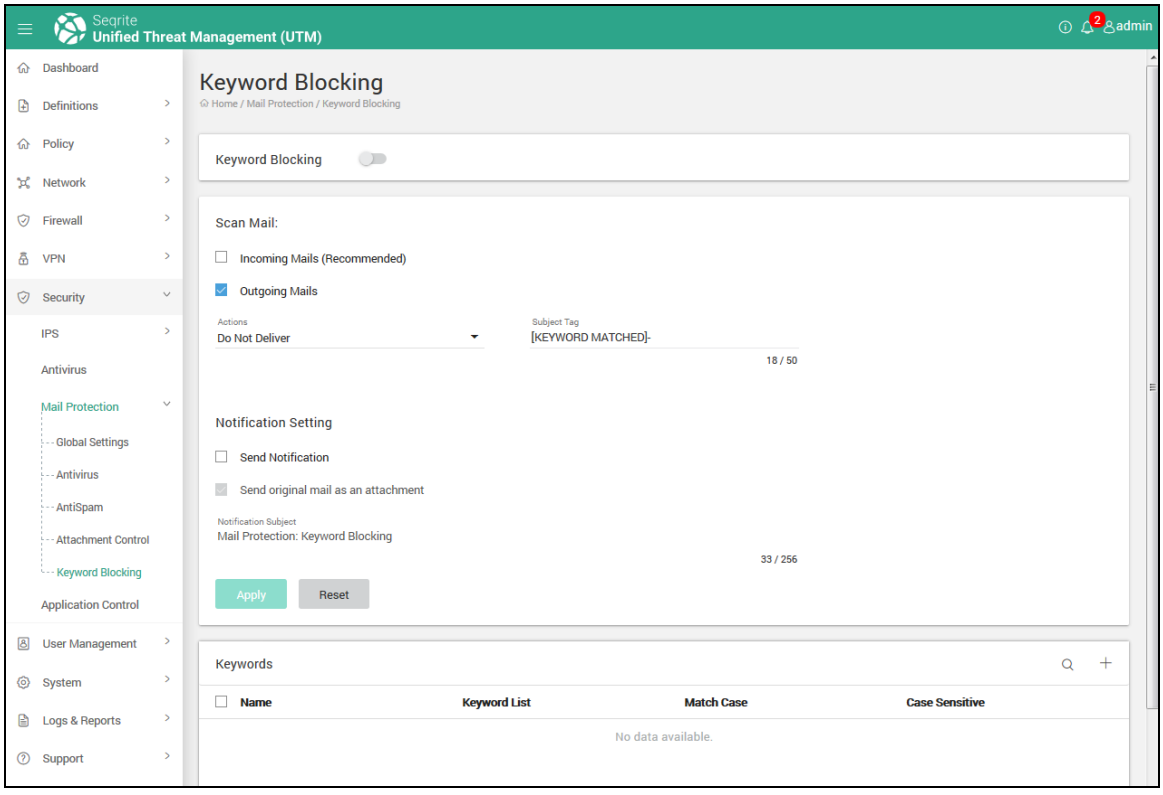
Keyword Blocking

Email content filtering performed on the body and subject of an email helps provide an in-depth approach to email filtering. Encoded content can be used to hide malicious command that may control the communications originating and intended for the network. For example, a command to an implant can be encoded and inserted into the email's body. If such encoded content is detected the email should be blocked.

The keyword blocking feature will identify the string of characters like a word, number, or an acronym which may be present in subject or body of the email and used for malicious communications. Using the Keyword blocking feature you can choose to block email that contain the specified keyword.

Configuring keyword blocking

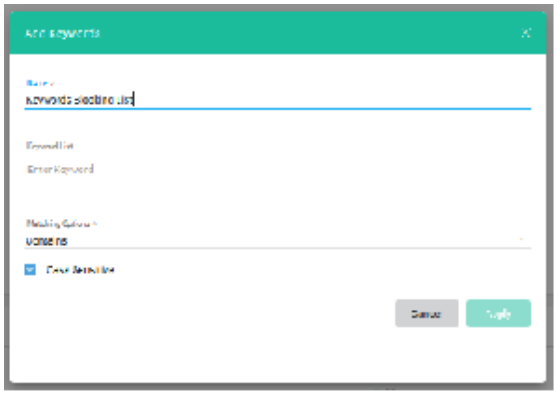
1. Navigate to **Security > Mail Protection > Keyword Blocking**. The Keyword blocking page is displayed.



2. Toggle the Keyword blocking status button to enable the feature.
3. In the Scan mail section, select the option to scan incoming or outgoing mail as required.
4. Select **Action** to be taken on the email which has the specified keyword:
    - Send Original: Sends the original email.
    - Do Not Deliver: If the specified keyword is found the email will be blocked.
5. In the **Subject Tag** field, enter a subject for the scanned email. This is appended to mail and sent to the recipient. For. e.g. Keyword Matched.
6. In the Notification Settings section, select the Send Notification option to send a notification to the administrator. The option for sending original email as an attachment is selected by default.
7. In the Notification subject textbox, you can add a Notification Subject, for e.g. " Mail Protection: Keyword Blocking", this text will be appended to the subject line of the mail.
8. Click **Apply** to save the keyword configurations**.**

Adding keywords to the blocking list

1. Navigate to **Security > Mail Protection > Keyword Blocking.**
2. In the Keywords section, click **+ (Add)** to add keywords that need to be checked in emails for blocking.



3. Enter the name of the list, the keywords that need to be checked for blocking the email and the matching options, whether starts with, ends with, complete word, or contains the keywords.
4. Select the option for case sensitive check if required.
5. Click **Apply** to save the keywords configuration.

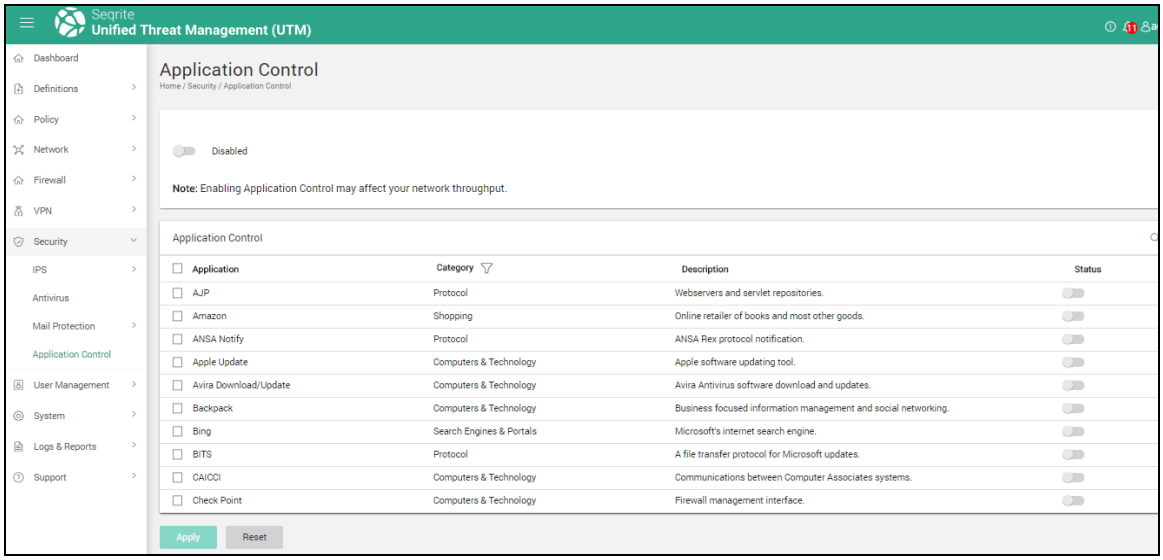
Application Control

Application Control feature on Seqrite UTM helps in restricting insecure and low productivity applications from monitored network environments thus saving on Internet bandwidth

consumption. It provides a database of 1700+ applications which network administrators could block. These applications may be web based or standalone applications. In addition, these activities are logged which helps to keep a track and trace the activities.

Configuring application control

1. Navigate to **Security > Application Control**. The Application Control screen is displayed.



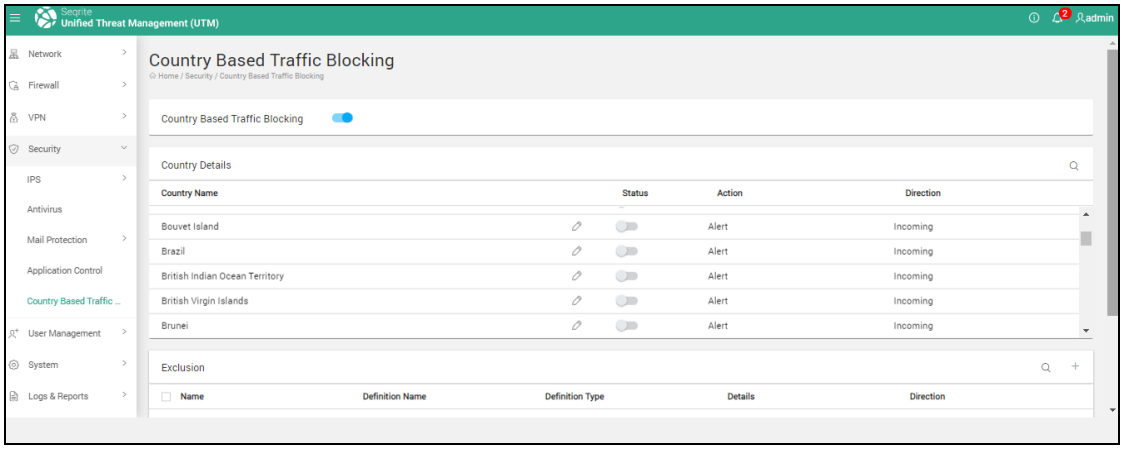
2. Application control is disabled by default, toggle the status button to enable.
   Note: Enabling application control might affect your network performance.
3. By Default, all the controlled applications are allowed. Select the application name which you want to block.
4. Click **Apply**. The selected applications will be blocked on the Seqrite UTM network.

Country Based Traffic Blocking

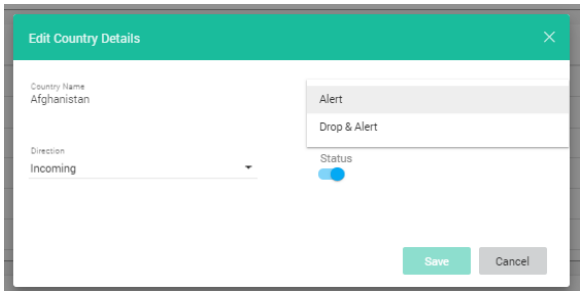
You may need to block network traffic to and from certain countries that are known to be sources of cyber-attacks. Some geographical regions may harbor individuals who carry out repeated brute force login attacks on your network and may need to be blocked. You also might want to prevent users in your computer network from accessing these networks. Seqrite UTM allows you to block all incoming traffic from and towards these countries. Anonymous IP addresses are used to hide a web user's true IP address and misrepresent their geolocation deliberately by fraudsters and other bad actors. Users in computer networks also use anonymous IPs to bypass geolocation controls to access restricted media content not available in their country. You can also block traffic to and from anonymous proxy networks and satellite providers that are not bound to a specific country.

Configuring country-based-traffic blocking

1. Navigate to **Security > Country Based Traffic Blocking**.



2. Toggle and enable the Country Based Traffic Blocking status button.
3. In the country list, toggle the corresponding status button for a country from which you want to block the traffic from and to your local network.
4. Click the Edit button icon besides the status button to configure whether you want to alert or alert and drop the traffic from the designated country.



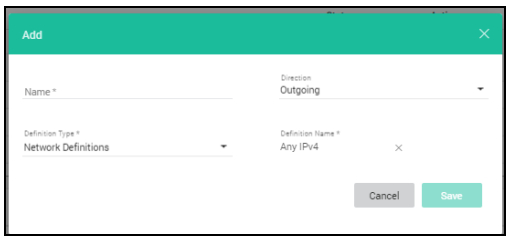
- If you select Alert, you will only be alerted on the dashboard if any traffic is sent to or comes from on the dashboard.
- If you configure the Alert and Drop option, all packets to and from that network will be dropped and alerts displayed on dashboard.

5. Select the traffic type, whether Incoming, Outgoing or both.
6. Click **Save.**

Creating exclusions for certain countries

You may need to exclude certain networks from certain countries from which you may have blocked network traffic. You can add these networks to your network definition list and add that definition to the exclusion list.

1. Navigate to **Security > Country Based Traffic Blocking**.
2. In the Exclusions area, click the + icon to create a new exclusion rule.



3. Enter a name for the rule.
4. Select the direction of the traffic that you want to block, whether incoming or outgoing or both.
5. Select the network that you want to exclude from Definition types available or create a new definition type using the + (Add) icon.
6. Click **Save**. The exclusion is saved and applied.

Chapter

11

User Management

You can create users, groups, and apply Internet access policies for groups using the User Management page. You can perform the following to control and restrict the use of Internet on your network:

- Create users and assign users to specific groups.
- Allow group-wise surfing along with limited access to Web sites.
- Assign different time slots for groups with restricted access rights.
- Allocate bandwidth usage to the users and groups. This feature allows you to keep a track of the bandwidth usage along with a statistical report on the same.
- Create your Internet traffic policies for network, define and restrict Internet access with the help of User Management features.
- Maintain organization rules and policies regarding Internet usage.
- Create and manage Guest user accounts and their Internet access.
- Allocate authentication servers for users.

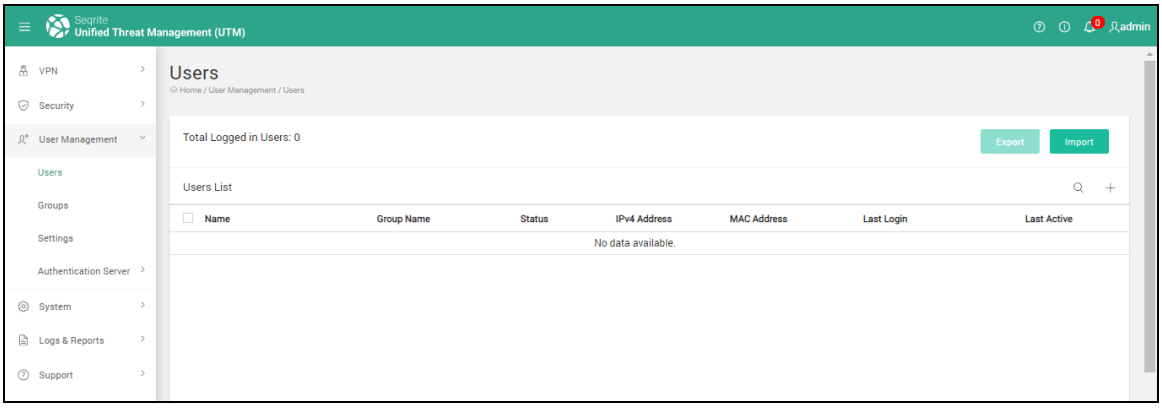
The User Management page is divided into following sections:

- Users
- Groups
- Guest User Settings
- Authentication servers

These sections help you to access further options under each section for configuration and management.

Users

The Users page allows you to manage users that is create, edit, delete users and allocate them to a particular group. Users can be created locally or imported from an Authentication Server or a .xls file. The Users page displays the details of the users, such as user name, group name, authentication, login status, and IP/MAC bind details.

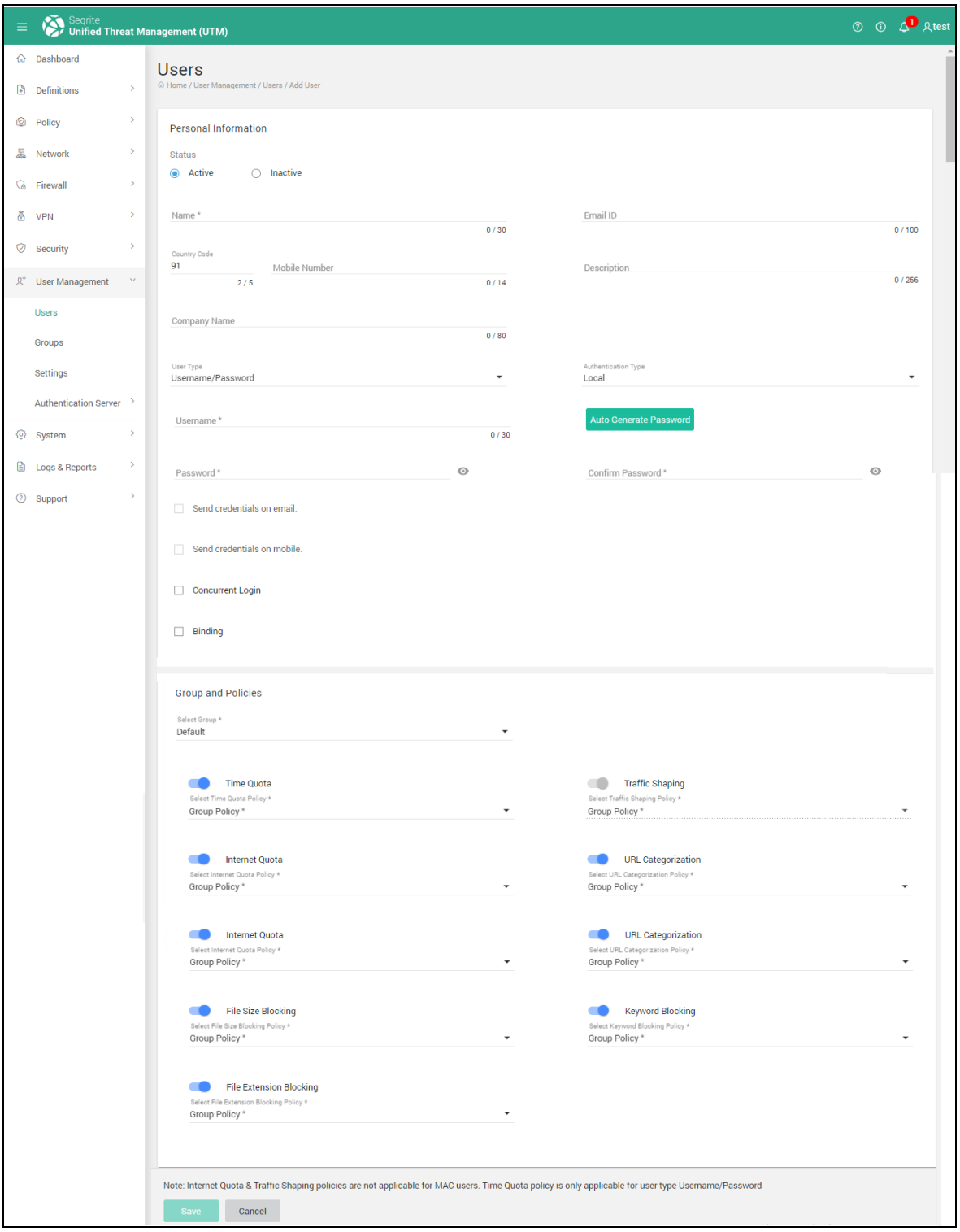


The following information is displayed about the users:

Field	Description
Name	Displays the logged users name
Group Name	Displays the group to which the logged in user belongs
Status	Displays the status whether, the user is in enabled state or disabled state. Disabled users cannot login and access the Internet.
IPv4 address	Displays the IP address associated with that user.
MAC address	Displays the MAC address of that user.
Last Login	Displays the time when the user last logged in.
Last Active	Displays the time when the user was last in active mode.

Adding a user

1. Navigate to **User Management > Users**. The Users management page is displayed.
2. Click the **+ (Add)** icon on upper right corner. The **Add Users** screen is displayed.



3. Set the status for the user whether active or inactive.
4. Enter the user's name, email address, country code, mobile number, description and company name if applicable.

5. You can select the user type, whether combination of username and password, or IP address.

   - If you select user type as Username/Password, the follow options as shown in the table are displayed, configure as required.

Field	Description
Authentication type	Enables you to select the authentication method, whether local or through Authentication Server (Active Directory or LDAP). If Local is selected, then the user is created locally that is username and password is stored on Seqrite UTM. Note: If the user is authenticated through Authentication Server then, the username must be identical to the username on the Authentication Server.
Username	Enter the desired username.
Password	Enter a password. Password should be alphanumeric and between 6 to 20 characters in length and contain least one special character. You can also use the Auto Generate Password option to generate a password.
Send credentials on email	Use this option to send the authentication details to users on email
Send credentials on mobile	Use this option to send the authentication details to users on mobile
Concurrent Login	Use this option to allow users to simultaneously login from multiple system. You can set the maximum number of concurrent logins that can be allowed to be Unlimited or Custom. If you select the custom option, then you can set a value for the maximum number of concurrent logins.
Binding	Use this option to bind the Username to a particular IP address or MAC address or both as required. You can bind multiple users to a single MAC IDs or IP address also. Note: If you bind a user with IP or MAC address, then that user can login only from the system having the configured IP or MAC address. You can bind the user with IPv4, IPv6, or both addresses.

If you select user type as IP Range, then 2 field options are displayed, 'From IP Address'

& 'To IP Address'. Enter the required information. .

Field	Description
IPv4 Address	Enter the applicable IP address if in IPv4 format.
IPv6 Address	Enter the applicable IP address if in IPv6 format.
Mac Binding	Select this option to bind the IP address to a particular device. Enter the MAC ID of that device.

6. If you select user type as MAC address, then a field to enter the MAC address is displayed, enter the corresponding MAC address in the field. In the groups and policies section, select the applicable group for the above user.

7. In the Groups and policies section, configure the following options for the various policies as required:

- Select Group: This section allows you to select group for a configured user from the drop-down box.
- Policies: This section allows you to select particular policy for a configured user. Default setting is Group Policy. You can choose and assign policy from drop-down box.
    - Group Policy: If user is a part of Default group, then all the policies applied on Default Group will be applicable on user.
    - Custom Policy: You can select another policy from drop-down and assign the same. The drop-down will show all the pre-configured policies.
    - No Policy: In case you want to exclude a user from any policy assignment then toggle the status button for that particular policy to disable that policy for that user.

8. Click **Save**. The new user will be created and displayed in the list on User management page.

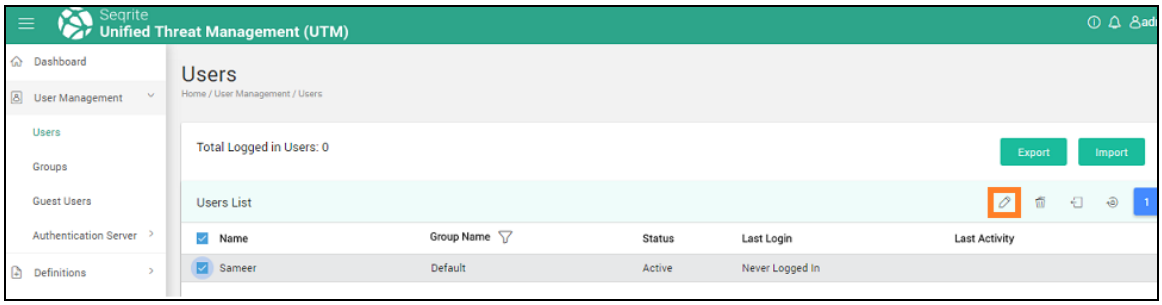
User Type Policy permissions table

Policy Type	Whether applicable to			
	IP-Wise users	IP range users	Name-wise users	MAC address users
Content Filtering	Yes	Yes	Yes	Yes
Internet Quota	Yes	Yes	Yes	No

Time Quota	No	No	Yes	No
Keyword Blocking	Yes	Yes	Yes	Yes
File size Blocking	Yes	Yes	Yes	Yes
File extension Blocking	Yes	Yes	Yes	Yes
Traffic shaping	No	No	No	No

Editing a User

1. Navigate to **User Management > Users**.
2. Click on the Edit icon (highlighted) of the User Name in the list given on the Users page.



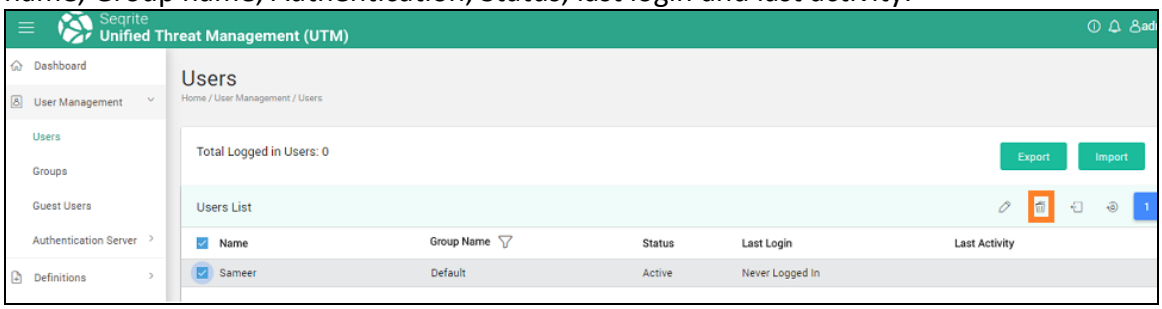
3. Make the required changes in the User details.
4. Click **Save**.

   Note: User name cannot be changed while editing a user.

   If you are selecting a different internet quota policy, then you can either select to reset the previous data usage or continue with the previous data usage. For e.g. A user is assigned a policy of daily 100 MB internet usage and the user has used 70 MB of data. While editing if a new policy is selected, then resetting the previous data usage will clear the 70 MB usage.

Deleting users

1. Navigate to **User Management > Users**. The page displays the list of the users with the User name, Group name, Authentication, Status, last login and last activity.



2. To delete a user, select the user and click the Delete icon as shown in the screenshot.

   Note: You can also select multiple users for deletion.

Importing users

You can add users by importing the details from an excel sheet.

1. Navigate to **User Management > Users**. The Users management page is displayed.

   The Users management page is displayed with a list of the users with the User name, Group name, Authentication, Status, IP MAC binding status, and Content filtering status.

2. Click **Import**, the Import Users dialog box is displayed.
3. Select the applicable group.
4. Click **Browse** to browse and select the excel file containing the user details. The excel file must have been exported earlier using the export button. You can also create a new excel file and enter the details manually.
   Data should be in the following format:

   First Username,Password,Password Encryption value.

   The Password Encryption column must have a value 0 or 1. If password encryption is 0 then the password is in clear text. If password encryption is 1 then the password is encrypted.
   Note: If you are entering the details manually, set encryption type to 0, and enter the password in clear text only. Your spreadsheet should contain the data in comma separated values in a single column. The first row of spreadsheet contains column description, and will

be ignored at the time of importing.

	A	B
1	User Name,Password,Encryption Type	
2	User1,Test$123,0	
3	User2,Test$123,0	
4	User3,Test$123,0	
5	User4,Test$123,0	
6	User5,Test$123,0	
7	User6,Test$123,0	
8	User7,Test$123,0	
9	User8,Test$123,0	
10	User9,Test$123,0	
11	User 10,Test$123,0	

5. Click **Import**. The Import Users dialog box displays a message about the successful addition of users. These users will be listed in the Users list.

Exporting users

1. Navigate to **User Management > Users**. The Users management page is displayed by default.

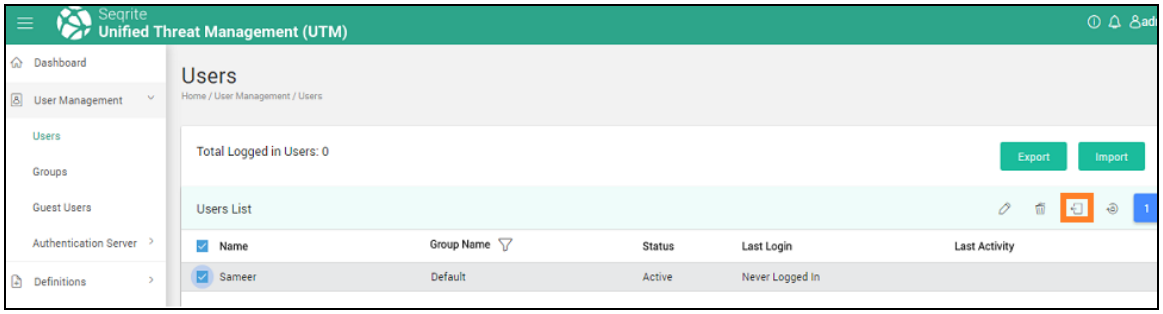
   This page displays the list of the users with the User name, Group name, Status, Last login and last activity.

2. Select the users whose details you want to export to excel sheet, click **Export**. The Export user dialog box is displayed.

3. In the Export Users dialog box, select whether you want to encrypt the Users password or not, and click **Export**. An MS-Excel file exported_users.xls containing the user details is downloaded on your computer.

Logging out a user by force

1. Navigate to **User Management > Users**. The Users management page is displayed.



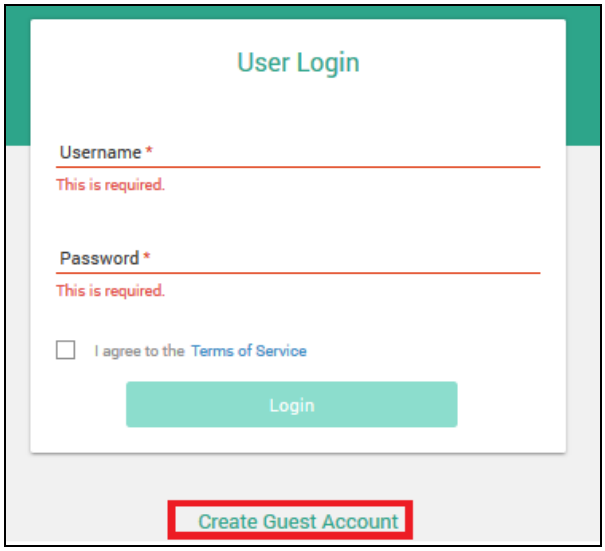
This page displays the list of the users with the User name, Group name, Status, Last login and last activity.

2. Select the User name and click the **Logout** icon as shown in screenshot (highlighted in red). The user is logged out of the network.
   Note: You can also select multiple users for logging out by force.
   Note: Settings for Force Logout of groups will override global settings for users under **User Management > Settings > Global Force** Logout.

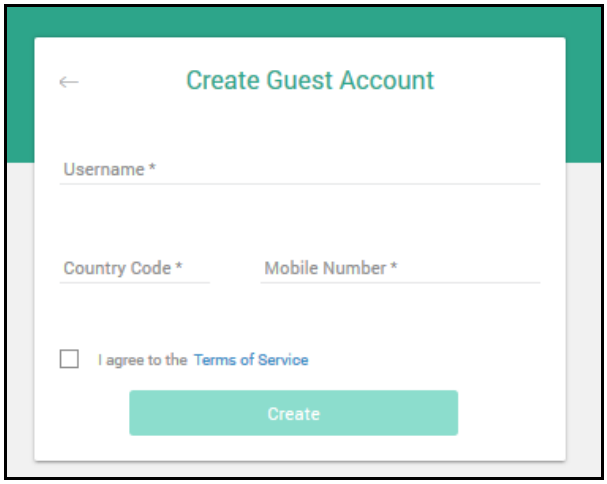
Creating a Guest user

Any user can create a Guest user if the Guest User link has been enabled by the Administrator for the users.

1. Enter the user login link in the browser address bar, for e.g. http://172.18.36.10/login.html#/dashboard. The login page is displayed as follows:



2. Click the Create Guest Account link.



3. Click **Create.** The Guest user is created and added to the Guest group by default.
4. The Guest user account will have a user validity defined as per the Guest group by the administrator.

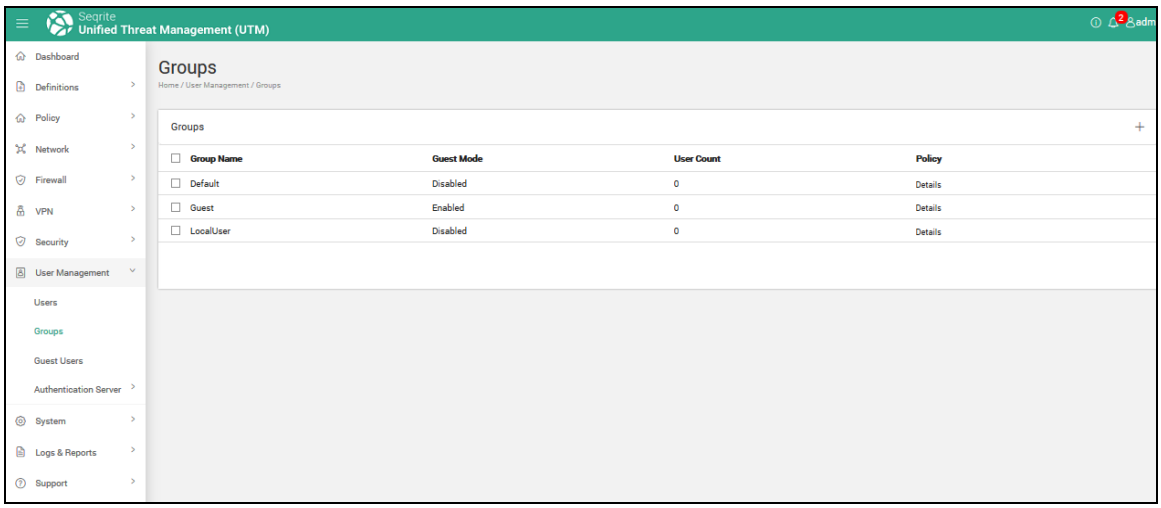
Groups

Group is a collection of users that have same policies for accessing Internet. Using the User Management section, you can perform the following functions on a Groups.

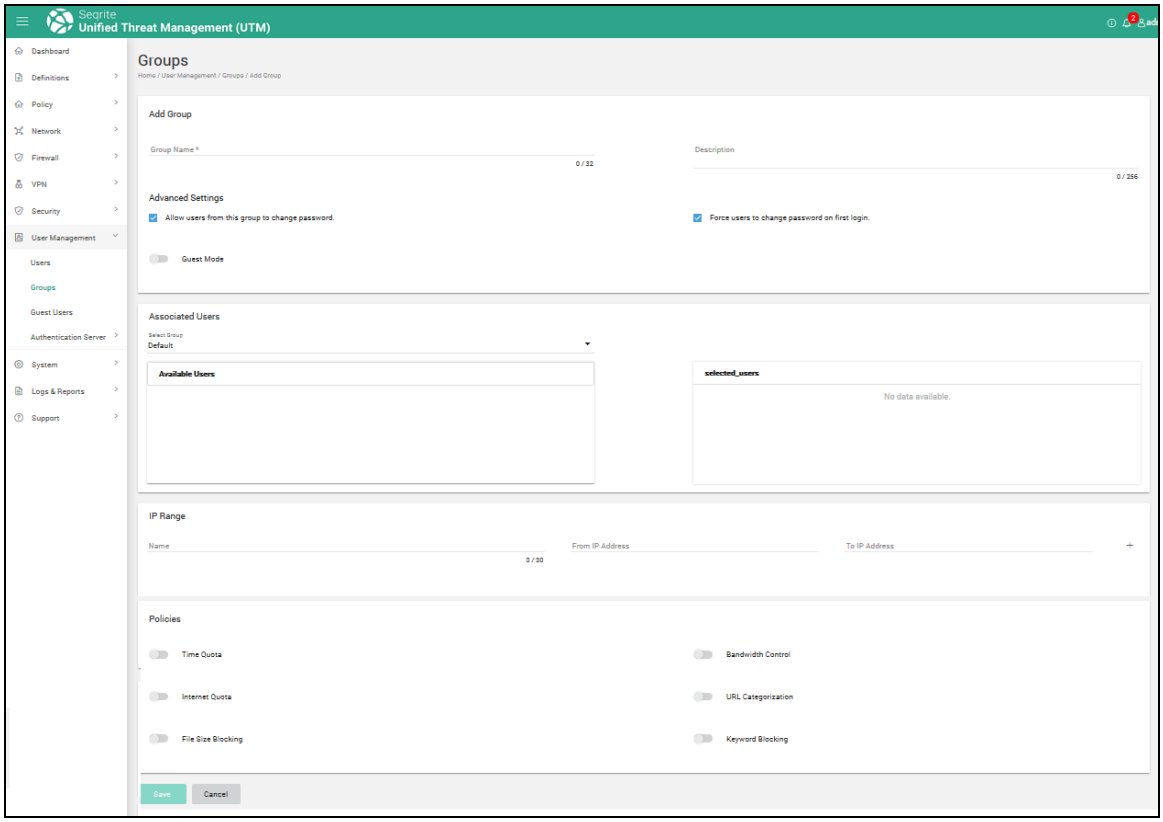
- Add a group when you want to specify a new group with new policies.
- Delete a group when you no longer want to use the group policies for users.
- Delete multiple groups when these are not required.
- Search for a group when you want to see details about the group.
- Apply Internet access policy, whitelist / black list Web sites for the group.
- Force Logout a user based on Time slot or duration.

Adding a group

1. Navigate to **User Management > Groups**. The Groups page is displayed with details of groups such as Group name, Guest mode whether enabled, number of users, and details of applied policy.



2. Click the +(**Add)** icon to add more groups.



3. Enter the group name and the relevant description.
4. Under Advanced settings, select the option to Allow users from this group to change password if required. You can also force user to change their password at first logon by enabling the designated option.
5. Enable the Guest mode if required. If enabled, configure the following options:

- Enter the maximum number of users allowed in the group.
- Select the Auto Purge after expiry option to delete users after expiry.
- Set the user validity time in days and hours as required.

Note: You can enable Guest User mode only when you create a group, later you cannot edit group to enable Guest User mode.

6. Enable the Force Logout option if you want to forcefully log out users of this group based on configured time slot or by duration. If you select Force Logout by Time, select the time after which users are logged out by force. For Force Logout by Duration, specify the number of hours after which the user members of this group will be logged out. Note: Settings for Force Logout of groups will override global settings for users under **User Management > Settings > Global Force Logout**.
7. In the Associated Users section, select the required groups and the associated members. To remove any member, select the member and click the delete icon.
8. In the policies section, configure the options for the following policies as described in the table:

Field	Description
Time Quota	Lets the user access Internet as per the setting in the applied policy.
Internet Quota	Allows you to set the internet access limit for users of the group. The following options are available: **Disabled:** Provides unrestricted data usage to the users of the group**.** **Enabled:** Allows you to select Internet access policy from the given dropdown.
File size blocking	File size Blocking Restricts upload or download as per the file size configured in the applied policy.
File extension Blocking	You can block files by specifying the extension type.
Traffic Shaping	Use Traffic Shaping to can create policies that restrict the bandwidth for users and groups based on protocols.
URL Categorization	Enable URL categorization and select the applicable policy that you want to apply for new group. Note: URL categorization for group will work only if the URL Categorization is enabled in Content Filtering. (See URL Categorization for more information)
	Domain wise: Use the Add button to add domains that the user can browse safely. To remove a domain from the list, select a domain and then click **Remove** on the upper right side. Note: If you select this option, then only the domains added in the list will be allowed for that group and all other Web sites will be

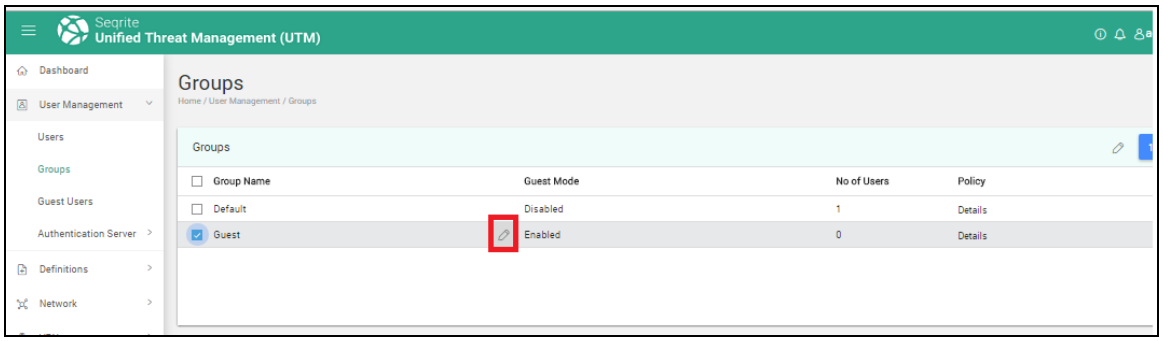
Field	Description
	blocked.
Keyword Blocking	Blocks network traffic if it contains words that are defined in the applied Keyword blocking policy.

Note: You must create the policies before you can apply them to groups.

9. When you have finished configuring all the above options, click **Save**.

Editing a group

1. Navigate to **User Management > Groups**.
2. Select the **Group Name** in the list given on the Groups page and click the Edit icon that appears (highlighted in red). The Edit group page is displayed.



3. Make the required changes in the Group details.
4. Click **Save**.

Note: Group name cannot be changed while editing a group. You can enable Guest User mode only when you create a group, later you cannot edit group to enable Guest User mode. If you are selecting a different internet quota policy, then you can either select to reset the previous data usage or continue with the previous data usage. For e.g. The users of a group are assigned a policy of daily 100 MB internet usage and the user has used 70 MB of data. While editing if a new policy is selected, then resetting the previous data usage will clear the 70 MB usage.

Deleting a group

1. Navigate to **User Management > Groups**. The Groups page is displayed with details of groups such whether guest mode enabled, number of users, and applied policies.
2. Select the group that you want to delete and click the **Delete** icon on the upper right side to delete the selected group. You can select multiple groups at a time for deletion.

Note: If a group is deleted, the users are assigned to the Default Group. Default and Guest group cannot be deleted.

User Settings

In this section you can configure the settings for the users as well as the Guest users. You can enable a Guest User link to appear on the user's login page, so that they can create a guest user. You can also set the default password strength for both user types, users and Guest users.

A Guest User is a non-registered user who can be given default set of permissions to access the Internet through SEQRITE UTM for a particular time duration. After the validity of Internet access expires, the Guest user is not allowed to access Internet. You can also set to delete the Guest user automatically.

Note: The Guest User feature will be available only if you have purchased the SMS feature. .
Note: The Global Force Logout settings are applicable only for Name-wise users and are not applicable to IP-wise users.

Managing User Settings

1. Navigate to **User Management > User Settings**. The following screen will be displayed.

2. In the Guest User link section, enable the Guest User link to enable guest user registration on Seqrite UTM User logon screen.
3. Select Guest Parent Group. The Guest users that will be created through the link will be added under the selected group.
4. Set the password strength as required. If you select strong password, the password set should be a combination of lowercase & uppercase letters (not starting with word admin), numbers and special characters from !^&$*()%+{}?<>| and its length should be at least 8 characters.

5. Select Global Force Logout if you want to log out users by force. If you select Force Logout by Time, select the time after which users are logged out by force. For Force Logout by Duration, specify the number of hours after which the user members of this group will be logged out.
   Note: Settings for Force Logout of groups under **User Management > Groups > Advanced Settings > Force Logout** will override global settings for users.

   Enable **Logout all users on reboot** option if you want to logout all users on server reboot. Users will then have to login again.

6. Click **Save**.

Authentication Servers

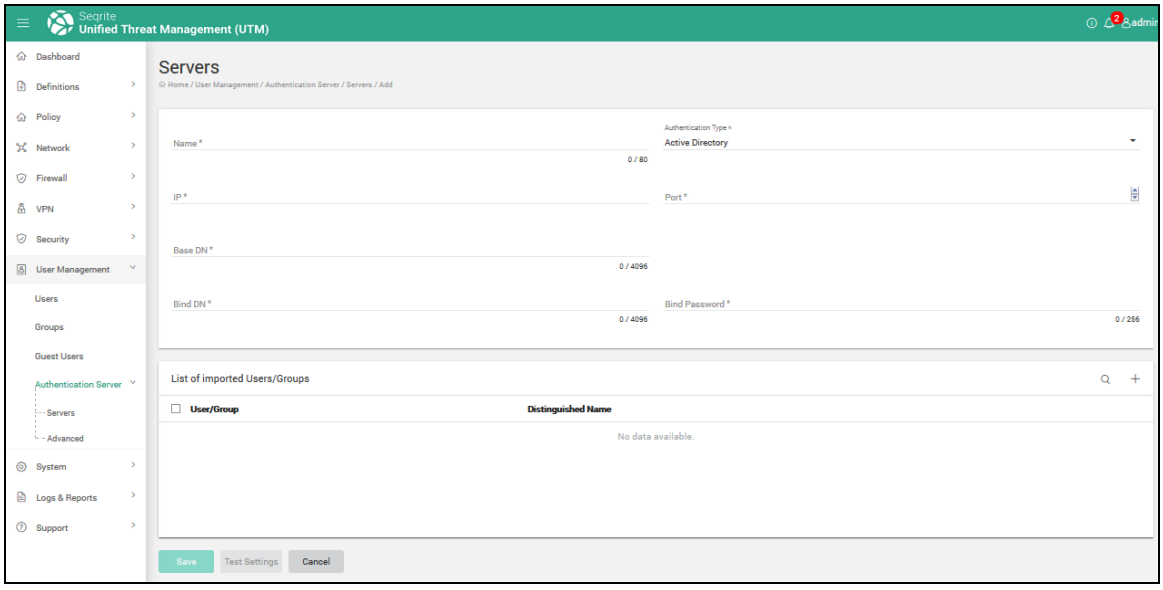
Authentication server is a server that provides authentication services to users or other systems via networking. You can register the authentication servers such as Active Directory for various groups and users in your network with the Seqrite UTM. You can also configure the synchronization cycle for Seqrite UTM to synchronize with the Authentication servers.

You can perform the following functions under this feature:

- Add /Edit authentication servers.
- Delete authentication servers.
- Synchronize Seqrite UTM with the registered servers.

Adding a new server

1. Navigate to **User Management > Authentication Servers**. A list of the registered servers is displayed with details of the IP address, Port, Type, Base DN, and the status.
2. Click **Add.** The server details form is displayed.



3. Enter the **Name** of the server in the form and enter the other details in the following fields as required. The table below explains the fields on the page:

Field	Description
Authentication type	Use this to specify the type of the Authentication server, whether LDAP, or Active Directory. Note: If LDAP is selected then Anonymous Login option is displayed.
IP address	Enter the IP address of the new authentication server.
Port	Enter the port number for accessing the server.
Base DN	Enter the Base Distinguished Name. The Base Distinguished Name is the starting point of the LDAP tree from where users or groups are to be searched. Note that the base DN must be specified by the full distinguished name in LDAP notation (For example, ou=internet,dc=example,dc=com).
Bind DN	Enter the Bind Distinguished Name used to authenticate the LDAP server (usually LDAP administrator), Bind DN should be in the format (CN=administrator,OU=accounts,DC=example,DC=com).
Bind Password	Enter the Bind Password that the Seqrite UTM will use for synchronizing with the Authentication servers.

4. In the list of imported users/Groups add/remove any users or groups as required.
5. Click **Test Settings** after you have entered all the details. The Seqrite UTM tries to connect to the registered Authentication servers and returns a successful message. Before you save the Authentication server details, you can import or delete groups of users.

   Note: If the authentication server status if OFF then import does not work.
6. Click **Save**.

   All the authentication servers added are displayed in the Authentication Servers list. A summary of Name, IP Address, Port, Type, Base DN, and status is displayed.

   If the status is ON then that authentication server is enabled and available for authentication. If status is OFF then that authentication server is disabled and not available for authentication.

Importing/Deleting users from configured Authentication Servers

1. Navigate to **User Management > Authentication Server > Servers**. A list of the registered servers is displayed with details of the IP address, Port, Type, Base DN, and the status.
2. If no servers are visible, click **Add** on the upper right side to add a server. A server details form is displayed.

3. Enter the name of the server in the form and enter the other details in the following fields as required.
4. In the List of imported Users/Groups, click **Import**. Seqrite UTM then connects to the configured authentication server and displays a list of the users and groups. You can use the Test Settings option to check if you can connect to the server.
5. Carry out the following action as required:
    i. To import groups into the Seqrite UTM, select the groups and click **Import**. Details of the groups along with the users are imported into Seqrite UTM.
    ii. To delete the groups, select groups and click **Delete**. The selected groups are deleted from Seqrite UTM.

Deleting Authentication servers

1. Navigate to **User Management** > **Authentication Servers**. A list of registered authentication servers is displayed with details of the IP address, Port, Type, Base DN, and the status.
2. Select a server that you want to delete and click the **Delete** icon. You get a confirmation prompt before the Seqrite UTM deletes the server from the list.
3. If you want the users associated with the server to be deleted, select the users and click **Delete**. The users associated with the authentication server are also deleted along with the server.

Synchronizing Seqrite UTM with the Authentication servers

You can synchronize the Seqrite UTM user list with the Authentication server to obtain the latest user list from the registered servers.

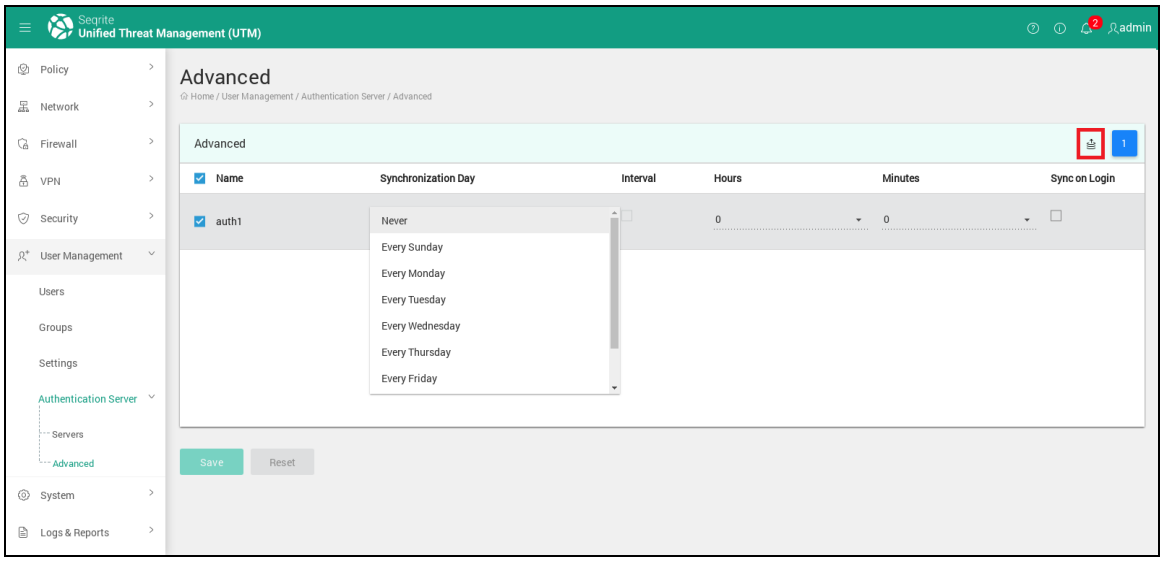
1. Navigate to **User Management**. > **Authentication Servers > Advanced**. A list of the registered servers is displayed with synchronization schedule.
2. Select a server that you want to synchronize with the Seqrite UTM, and click the **Update Now** icon. The Seqrite UTM user list is synchronized with the server user list.

Scheduling synchronization of UTM with Authentication servers

You can synchronize Seqrite UTM user list with the Authentication server to obtain the latest user list from the registered servers.

1. Navigate to **User Management > Authentication Servers** > **Advanced.** A list of the associated authentication servers is displayed.
2. Select a server that you want to synchronize with the Seqrite UTM.
3. Configure the synchronization day, and the hour and minute details for that server.

4. To repeat the synchronization at a particular interval, select the Interval option. UTM will synchronize with AD server as per the configured frequency interval.
   Note: For this option, synchronization can be set to happen at hours only. The minute option is disabled. For e.g., if you select synchronization day as Every Sunday, select the interval option and set the interval as 4 hours, then synchronization will happen every Sunday at 00.00 hours and repeat at 04.00, 08.00, 12.00, 16.00, 20.00, and last at 00.00 hours.



5. To enable synchronization automatically on login, select the Sync on login option.
6. Click **Save**. The Seqrite UTM user list will be synchronized with the server user list at the configured time.
   Note: To synchronize immediately, click the **Update Now** icon (highlighted in red box). The Seqrite UTM user list is synchronized with the server user list.

Chapter
12

System

High Availability

The High Availability (HA) feature in UTM 2.2 release ensures that the UTM appliance is available at all times and has in-built redundancy and reliable crossover. The feature actually utilizes 2 identical UTM hardware appliances in which passive appliance will takes over in case active appliance fails or develops a fault.

Note: The HA feature can be enabled on the T2 versions or higher configurations only.

Prerequisites

1. The hardware configuration of 2 appliances used for HA must be identical, that is it must be the same model. Both UTM appliances must be identical in terms of performance and load handling. Both the UTM appliances must have the same firmware version.
2. One interface on the 2 appliances must be linked by a direct cable (point to point connection) or through a switch for the HA dedicated link. For example: eth 2 interface on appliance 1 must be connected to interface eth 2 on appliance 2 only.

Working

There are 2 identical UTM devices, a primary and a secondary appliance that are configured in HA mode to enable the High Availability feature. The primary appliance normally operates in the active mode and processes all incoming and outgoing traffic based on the configured policies. The secondary appliance is meanwhile in Active- Standby (Passive) mode and does not process any traffic. A primary IP address is assigned to the primary appliance and a secondary IP address for the secondary appliance for each of the available interfaces. In addition, a virtual IP address is assigned to each interface. This IP address is maintained in case of any failover from primary to secondary and vice versa. The 2 UTM appliances check if the other appliance is alive as per the frequency defined for the heartbeat interval through the dedicated HA link. You can enable the watch status for each interface except the dedicated HA link to be monitored for failure.

Scenarios supported for HA failover

- System shutdown or reboot
- Interface (on watch) failure

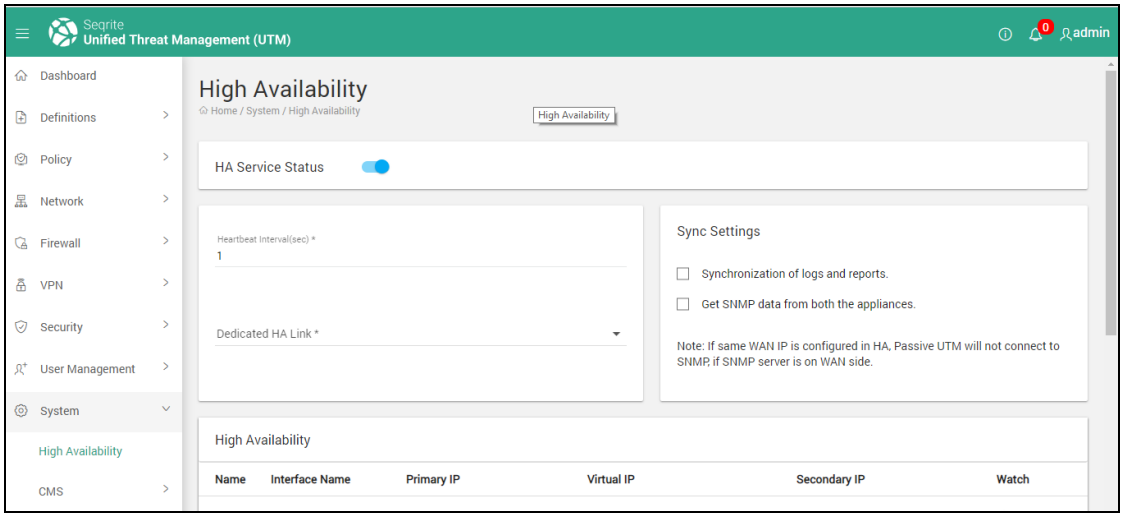
HA Status on dashboard

The following details related to HA are displayed on the dashboard:

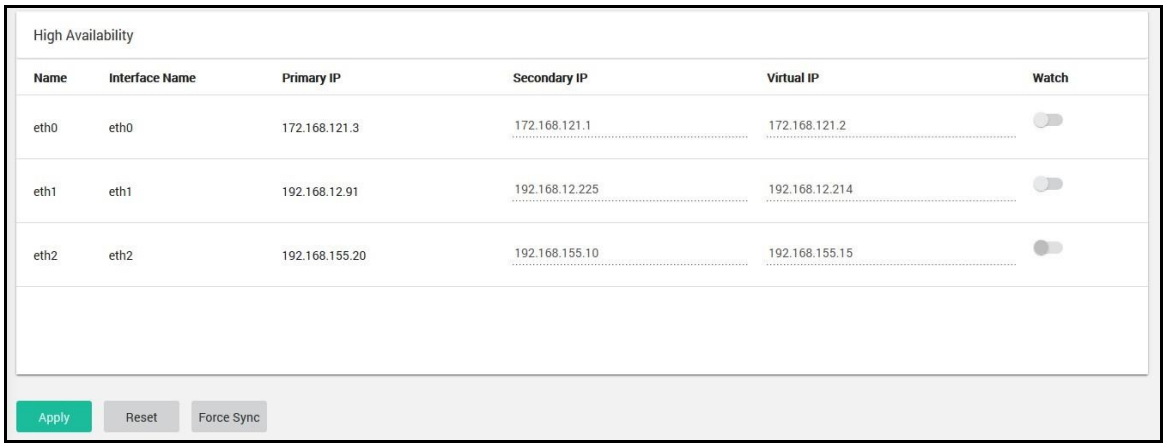
- Whether enabled or disabled
- The dedicated interface for HA link
- Heartbeat interval
- Status of 2 UTM appliances whether active, passive, fault or out of sync
- Firmware versions of the 2 UTM appliances

Setting up High Availability

1. Navigate to **System > High Availability** page.



2. Toggle the HA service button to enable the HA service.
3. Enter the heartbeat interval in seconds. This setting on the heartbeat interval decides the frequency at which the two appliances will check each other if active and alive.
4. Select the dedicated HA interface link from the list of interfaces in the drop-down.
5. Navigate to the High Availability interface settings. In the interface settings, the primary IP addresses are displayed for the available interfaces.



6. For each interface, enter the secondary IP address and the virtual IP address. The secondary IP address is assigned to the corresponding interface on the secondary appliance. The Virtual IP address is the actual IP address for the HA ready appliance for that interface.
   Note: The primary, secondary and the virtual IP addresses for each interface must be in the same IP address subnet class. For example, Primary IP: 172.168.121.3, Secondary IP: 172.168.121.4 and Virtual IP: 172.168.121.7
7. Toggle the watch button to enable the watch status for that interface. If you enable the Watch status, HA will monitor the interface for technical failure or hardware failure and then initiate a failover to the secondary UTM appliance.
   Note: You cannot put the dedicated HA link interface on watch.
8. Click **Apply** to save. To re-enter, click Reset and the previous values will be restored. The HA status will be updated on the dashboard.

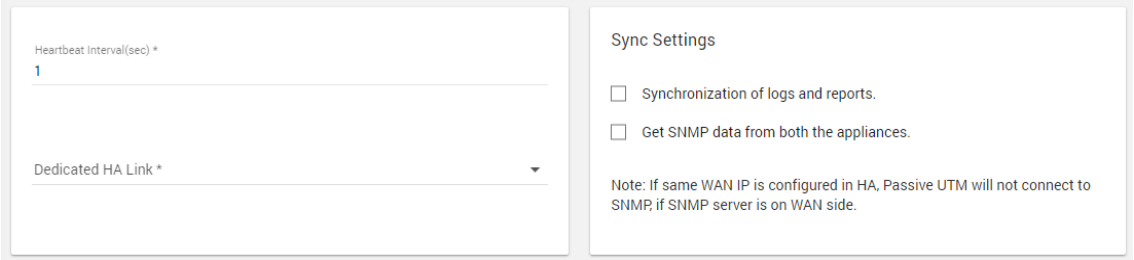
Synchronization between the 2 appliances

As the 2 appliances are configured in failover mode for high availability, data from the 2 appliances will have to be synchronized. Each time HA is turned from OFF to ON a configuration sync up is performed between the two appliances. You can also perform a forceful synchronization between the two appliances if peer appliance is in Out-of-Sync state to synchronize the following data on the two appliances:

- Interface configuration
- Definitions
- Policies
- Network settings
- Firewall settings

System

- VPN settings
- User Management settings
- Support
- Antivirus configuration settings
- IPS configuration settings
- Mail protection settings
- Application Control settings
- System parameters



- To sync logs (DHCP, VPN) & reports of both UTM appliances, in the Sync Settings area, select and enable Synchronization of logs & reports checkbox on HA page.
- To receive SNMP data of both the appliances on the SNMP server, in the Sync Settings area, select and enable the Get SNMP data from both appliances' checkbox on HA page.

  Note: If the appliances go in out of sync state, a banner will be displayed on the dashboard with a Force Syncup button. Click Force Syncup to complete the synchronization of the active and passive appliance.
  Note: The Force Syncup operation may take some time depending on the configuration, load and the user Interface will not be available till the operation is completed.

Centralized Management System (CMS)

Using the Seqrite CMS, you can now centrally view and manage your UTM appliances at different geographical locations. The CMS dashboard area displays the count for active licenses and expired license, count for licenses about to expire in a month.

The dashboard also displays widgets for the count of synchronized and unsynchronized UTM appliances. The dashboard also displays the count for viruses detected over the past 31 days, intrusions detected, and the policy breach attempts made by the users.

The count for the appliance by make is also displayed. You can also directly access the console of your registered UTM appliances through a Remote Access (RAC) link to manage the various UTM appliances.

Prerequisites

1. You need to buy the CMS license separately to avail of this feature. Contact your Seqrite representative for more information.
2. UTM software version must be 2.2 or higher.

Precautions to be taken during RAC session

- Do not change WAN IP during ongoing RAC session.
- Do not configure/modify HA settings during ongoing RAC connection.
- Do not change UTM web admin ports during ongoing RAC connection.

Note: Changing any of the above configuration would hamper RAC connectivity.

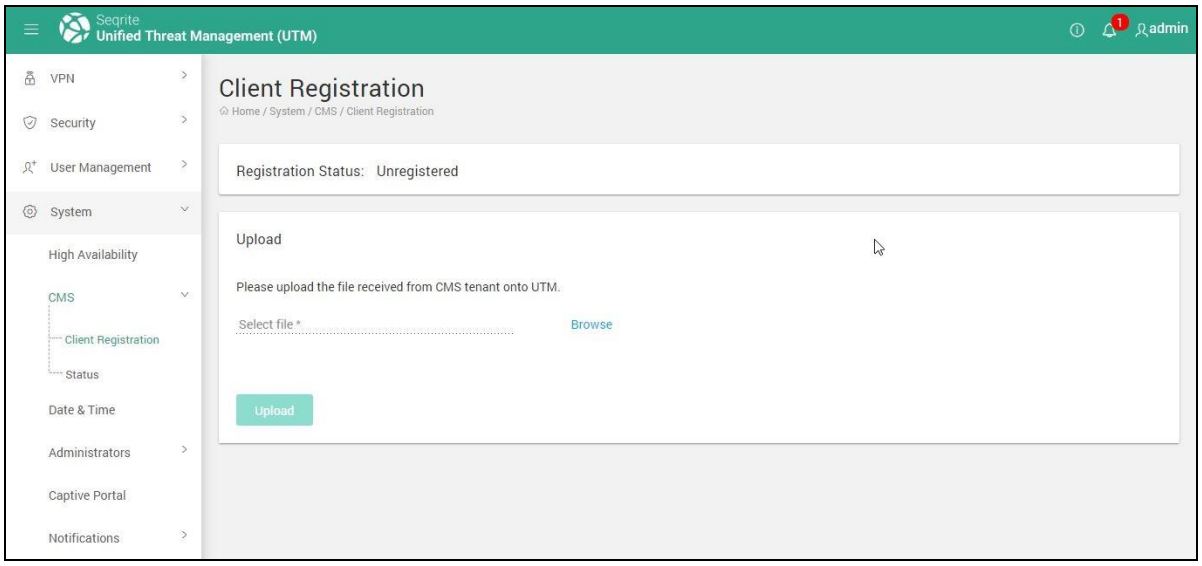
Working

After you purchase a CMS license, you will receive the login credentials through email. Using the credentials, you must logon to the Seqrite CMS portal that is cloud-based. In Seqrite CMS, on the Deployment page, the CMS administrator must create a deployment file for every appliance that must be registered with the CMS portal using the Create File button. The file can be downloaded to your computer and can be sent via email to the admin of the related appliance. The administrator needs to import the file into the console of that appliance and complete the registration process from the console of that appliance. For more information on creating the registration file, refer the user documentation for CMS.

Note: CMS support is disabled by default. It is automatically enabled after you register your appliance with CMS portal successfully. Your Seqrite support representative will share the CMS portal URL with you.

Registering with CMS

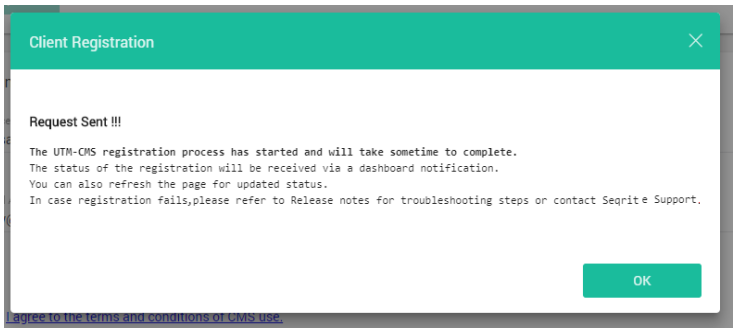
1. Logon to the dashboard of the UTM appliance that you wish to register with CMS.
2. Copy the deployment file on to your computer. The deployment file is sent by CMS admin and received by UTM administrator through email as an attachment.
3. Navigate to **System > CMS > Client Registration**. The status initially will be displayed as unregistered.

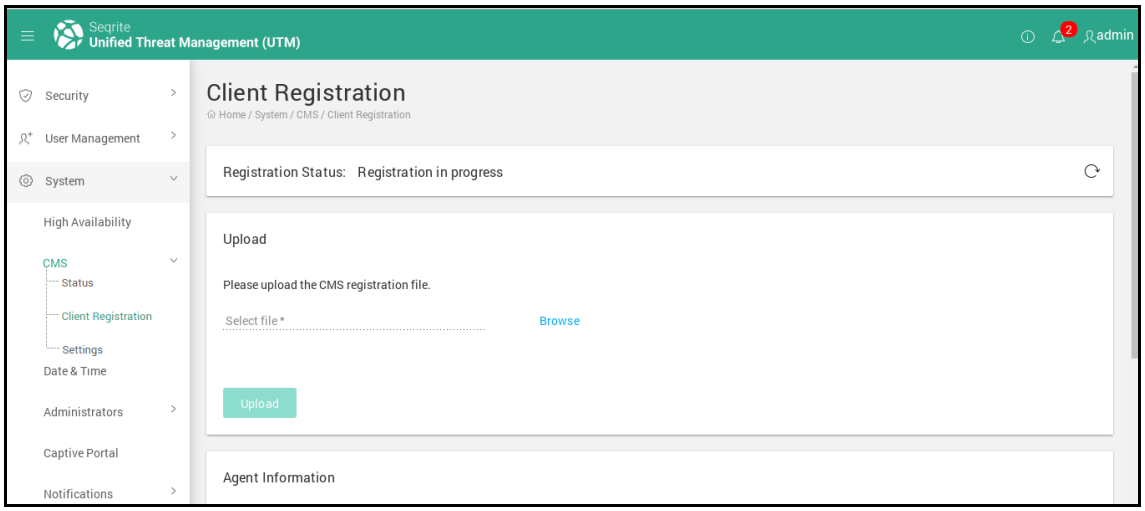


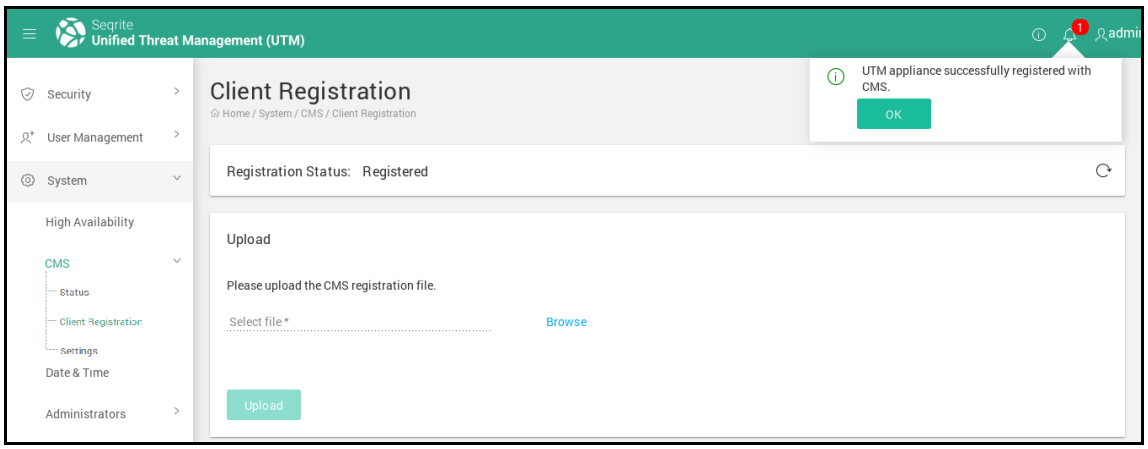
4. Click Upload to browse and upload the deployment file.
5. In the Agent information section, enter the device name. The other information is drawn from the deployment file.

6. Select and agree to the terms and conditions of CMS use.
7. Click **Register**. The success prompt is displayed, and CMS support is enabled for the appliance. A registration request will be sent to CMS. Once registration process is completed, an alert is

displayed via dashboard notification. You can also click the Refresh button on the upper right corner to check the current registration status.



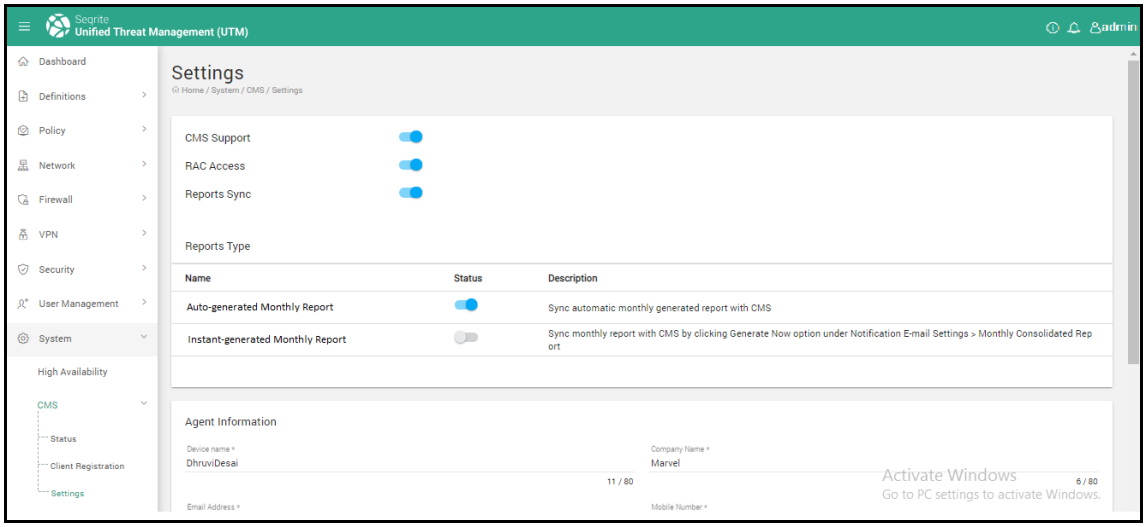




CMS settings

You can disable the CMS support, RAC access, and the synchronization of Reports from this page.

1. Navigate to **System > CMS > Status**. Initially the status for CMS support, RAC access and Reports Sync is disabled by default.
   Note: CMS Support is disabled by default. It is enabled automatically after you register your UTM appliance with CMS. You can disable the CMS support from this page if required. However, if you disable CMS support, the RAC access and CMS Reports synchronization will also be disabled.



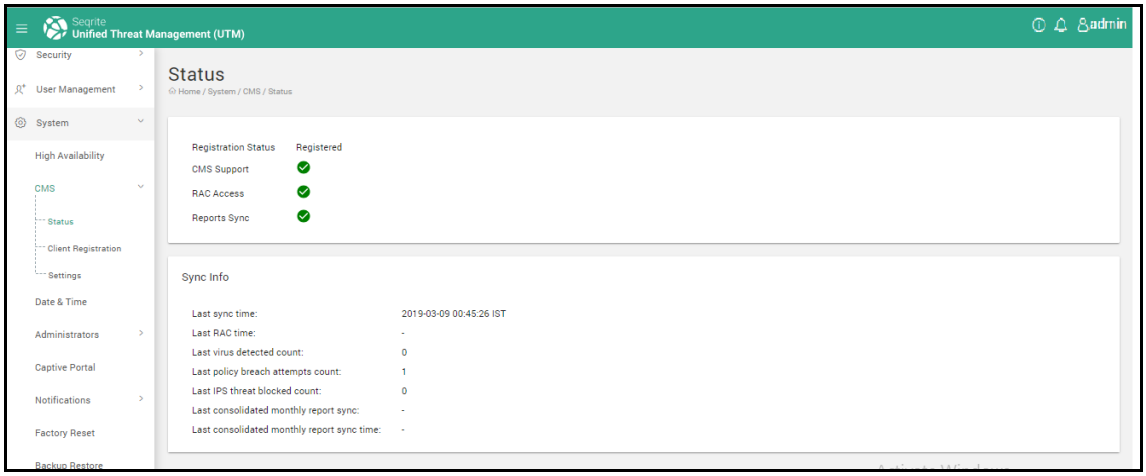
2. To change the sync settings for Report, in the Reports Type section, toggle the corresponding buttons for Auto-generated Monthly Report and Instant-generated Monthly Report as required.

Viewing the CMS status

You can view the status related to the CMS support, RAC access and Reports synchronization on this page. The synchronization information includes the last synchronized time, the last time RAC was utilized, the last detected virus count, last policy breach attempt count, last IPS threat blocked count, last consolidated monthly report sync status and the time.

System

1. Navigate to **System > CMS > Status**.

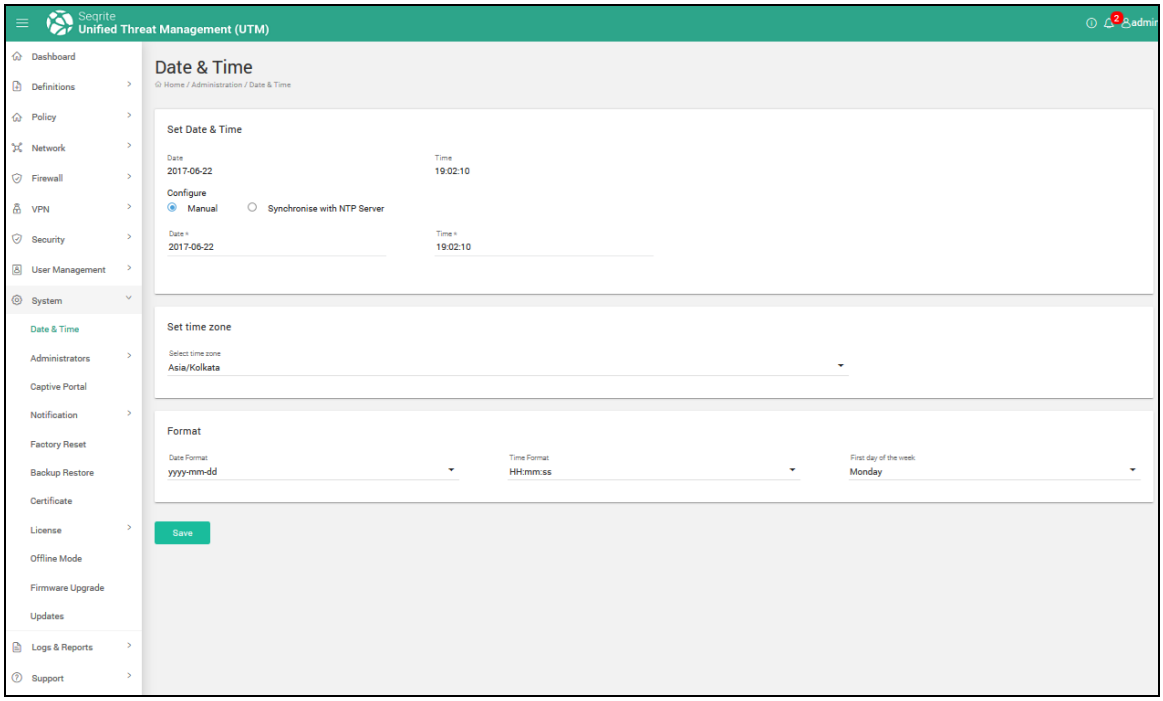


2. View the details as required.

Configuring the date and time

You can set the appliance date and time according to different geographical regions or synchronize with an NTP server.

1. Navigate to **System** > **Date & Time**.



2. The following table explains the fields on the page, configure as required.

Date	Displays the current Date of the appliance.
Time	Displays the current system time of the appliance.
Configure	Manual: Select the date and time from the dropdown. Synchronize with NTP server: Select this option to synchronize the appliance time automatically with an NTP server. Sync time using predefined NTP servers like asia.pool.ntp.org or in.pool.ntp.sorg or add new NTP server. Sync Now: Click this button to sync appliance clock with the listed NTP servers. The date and time will be synchronized with the NTP server having least time difference.
Time Zone	Select the time zone according to the geographical region in

	which the appliance is deployed.
Format	Set the Date, Time format and set the first day of the week.

3. Click **Save.**

Setting the time zone and format

1. Navigate to **System** > **Date & Time**.
2. Select the appropriate time zone and date format from the respective drop-down lists.
3. Click **Save**.

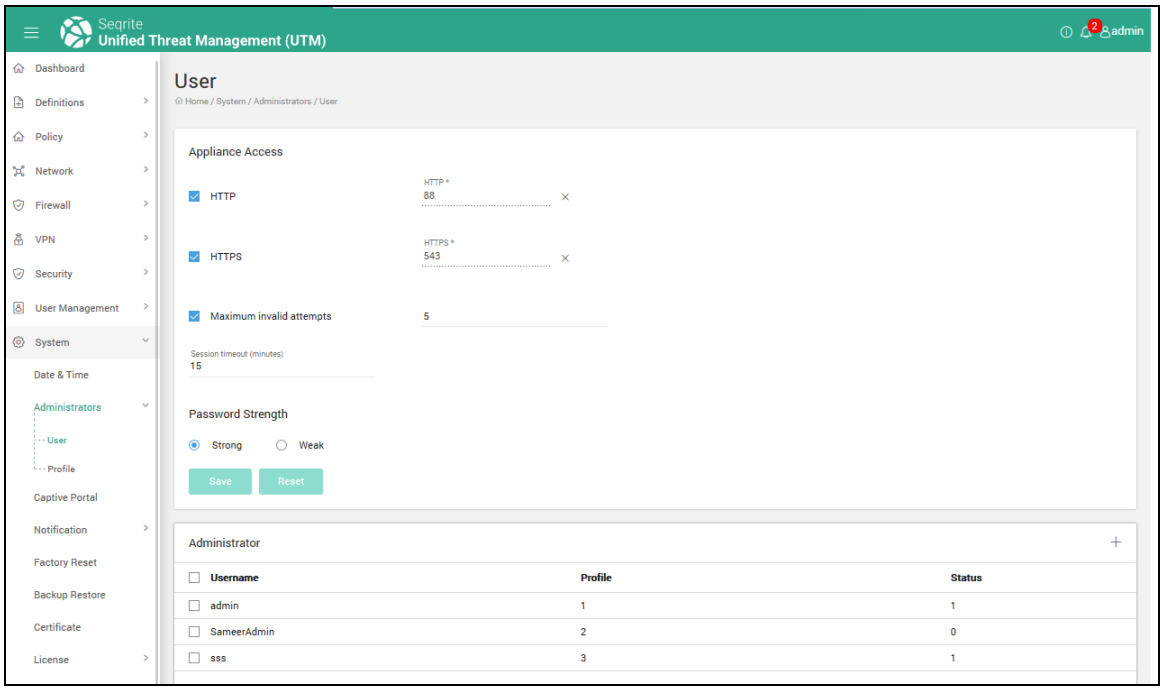
Note: Changed Date & Time will not be reflected in the previously created reports hence there could be inconsistency in the reports.

Administrator

The Administration page on the Seqrite UTM provides you the options for adding admin profiles, managing admin settings and SMTP settings. The Admin page lets you control appliance access over http or https ports, specify the maximum number of login attempts and specify the password strength for the administrator profiles.

Admin Settings

1. Navigate to **System > Administrators > Users**. The Admin page is displayed.



2. The following table displayed the available options, configure as required.

System

Option	Description
Http	Allows access over WAN on the specified ports and protocol
Https	Allows access over WAN on the specified ports and protocol
Maximum invalid attempts	Allows you to specify the maximum number of login attempts after which the account is locked out.
Session Time out	Allows you to specify the session time out parameter.
Password strength	Allows you to specify the password strength, whether weak or strong.

3. Click **Save.**

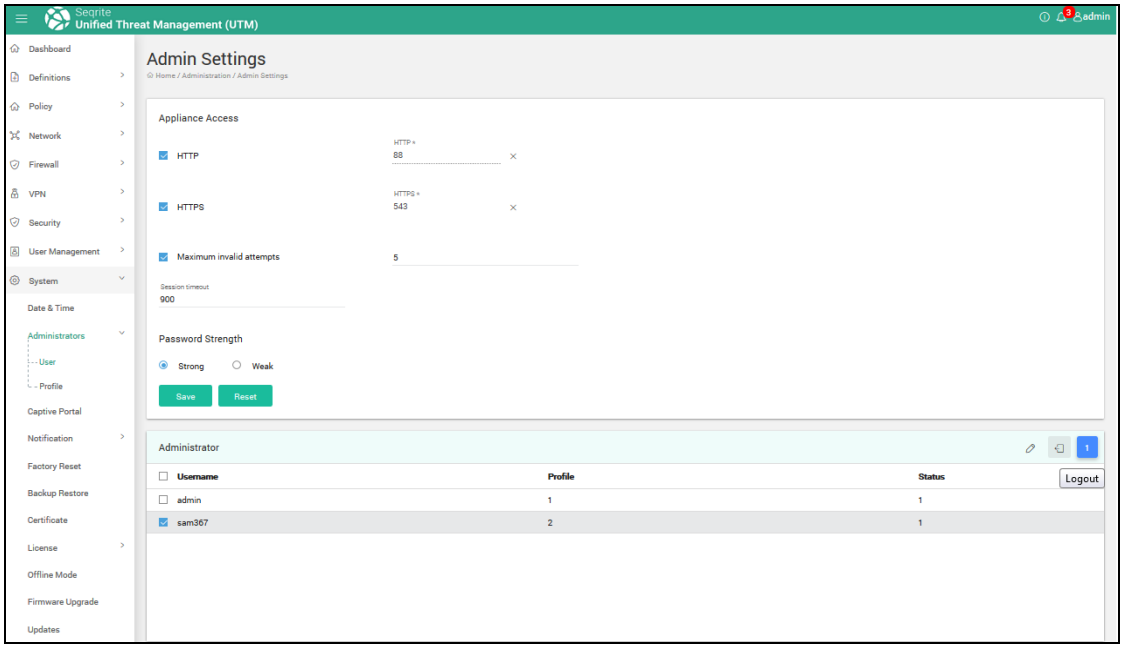
Adding Administrators

1. Logon to Seqrite UTM as Super Admin.
2. Navigate to **System > Administrators > Users**. The Admin settings page is displayed.
3. Click +(**Add) in** the Administrator List. The Add Administrator page is displayed.
4. Enter the user name and real name.
5. Enter the password for the new administrator. Confirm the password.
6. Select the type of admin profile to apply, whether Administrator with full rights or Read-only access.
7. Set the status, whether enabled or disabled.
8. Enter the email address, contact number and comments if any.
9. Click **Save.**

Deleting / logging out administrators

1. Logon to Seqrite UTM as Super Admin.

2. Navigate to **System > Administrators > Admin Settings**. The list of Administrators is displayed.



3. Select the admin user that you want to delete / log out, click **Delete/Log out** as required. The selected administrator is logged out forcefully.

Admin Profiles

This section allows to manage web Admin profiles. It provides definition of the rights Admin user can have. You can create, edit and delete Admin profiles using this section. There are three predefined Admin profiles:

Super Admin: This user type has full access to the portal and can make any changes in the System.

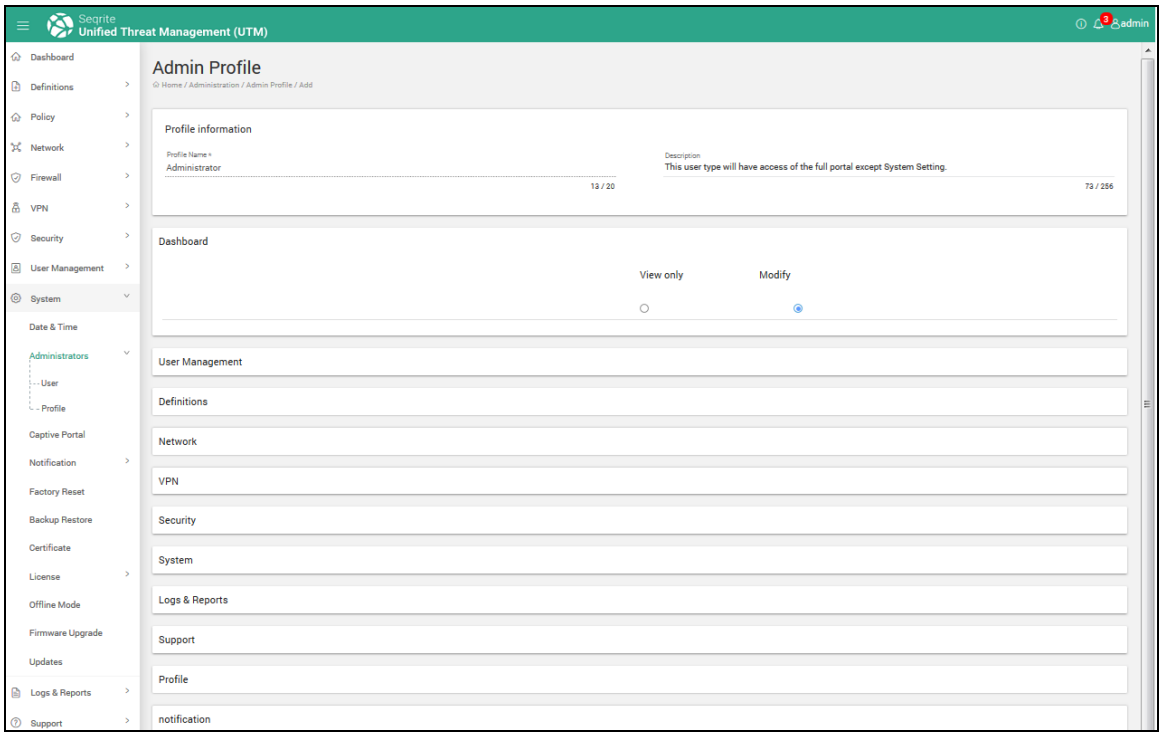
Administrator: This user type has full access to the portal except System Setting.

Read-only: This user type can only view everything in the web portal without being able to make any changes in the system like create, edit or delete.

Creating/Modifying Admin Profile

1. Logon to Seqrite UTM as a Super Admin.
2. Navigate to **System > Administrators > Admin Profile.**
3. Click +(**Add)** to add a new Admin Profile. The Admin Profile page displayed. To modify, select a profile from the list and click the Edit button that appears.

System



4. Enter a **Profile name** and description for the profile.
5. Configure the access permissions as required for each module. You can set the permissions to View only or Modify.
    - View only access allows user to only view the pages.
    - Read/Write access: Allows to make any changes in the system like create, edit or delete.
6. Click **Save**.

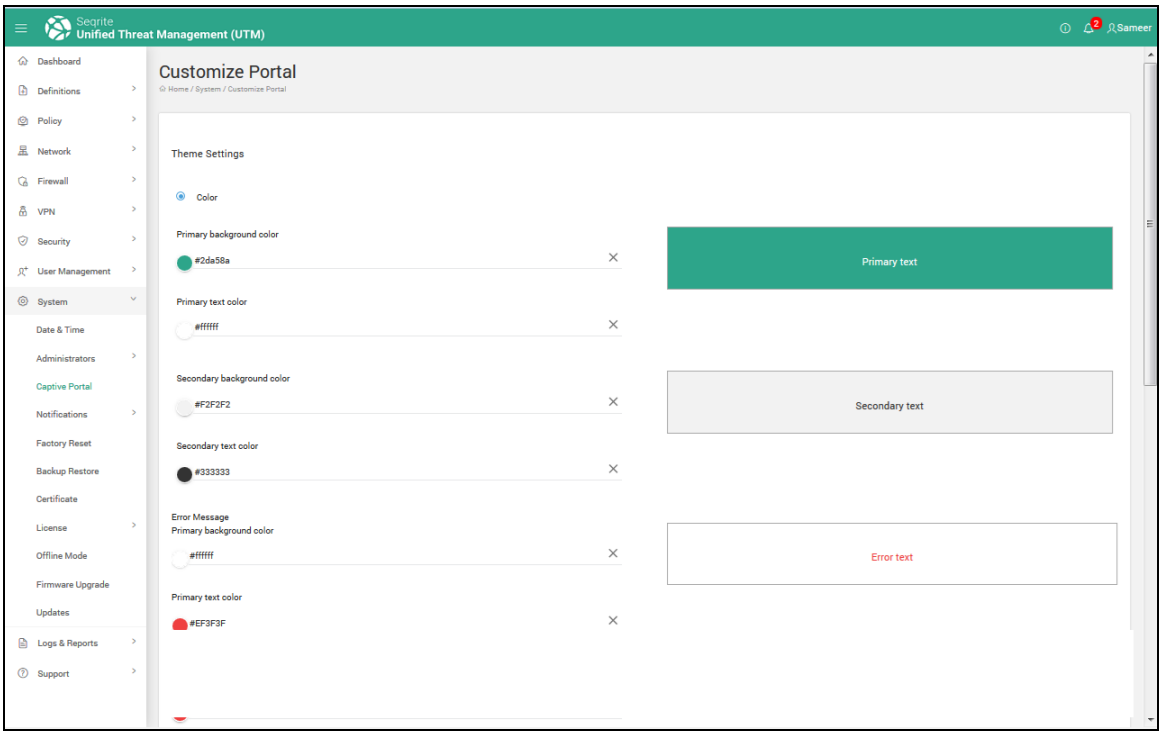
Deleting Admin Profiles types

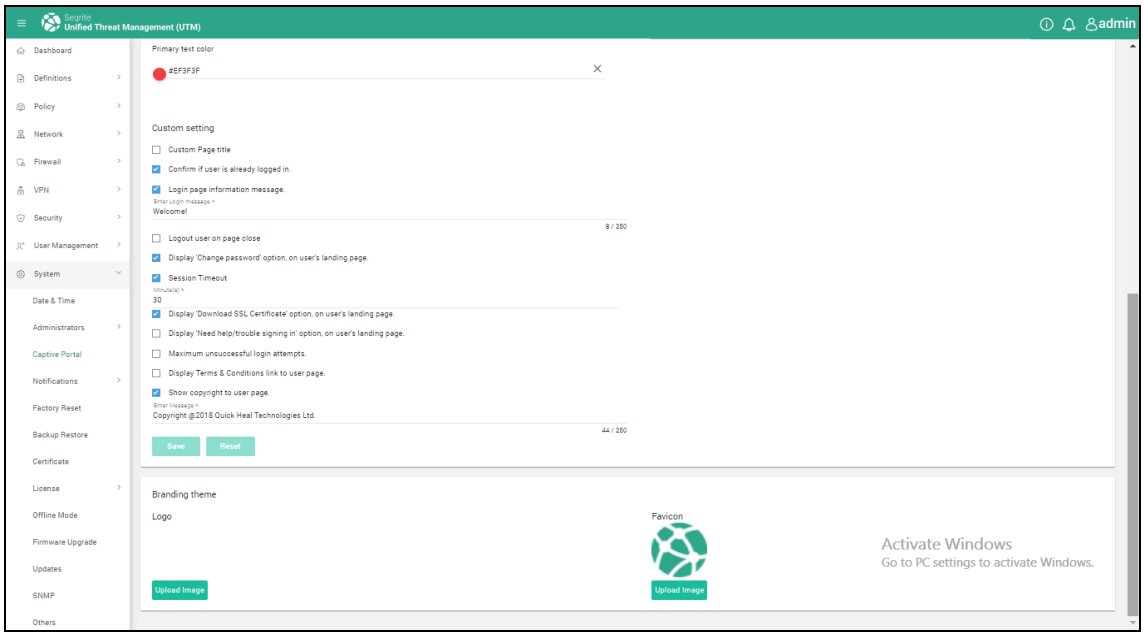
1. Log on to Seqrite UTM as a Super Admin.
2. Navigate to **System > Administrators > Admin Profile.**
3. Select the Admin profile that you want to delete, click **Delete**.

    Note: Deleted Admin profiles will be changed to Read-only user type. Predefined Admin profiles cannot be deleted.

Captive Portal (Customizing the web portal)

This feature allows you to customize Seqrite UTM web portal. The screenshot in two parts display the options that are customizable.





Customizing the web portal

1. Navigate to **System > Captive Portal.** The following table describes the options on the page.

Field	Description
Page Theme	Select the login theme page for your User login page from the available themes (Theme 1 and Theme 2).
Theme settings	Using this option, administrator can either set the theme by selecting the primary background color and text, secondary background color, primary text color, error message text and color or upload and image by selecting the Image option. Administrator can change the settings for Theme 1 and Theme 2, save them, and use as required.
Custom settings	Administrator can customize the following options as per requirement.
Custom page title	Using this option administrator can set page title.
Confirm is User is already logged in.	Using this option, administrator can allow a user multiple login and logouts with a confirmation message.
Login page information message. (Landing Page)	This message displays on login page before user logs in. For example, this can give an introduction about the site.

System

Field	Description
Logout user on page close	Administrator can log out a user if user closes a page. User will have to login again to access Seqrite UTM.
Display 'Change password' option, on user's landing page.	Administrator can display message asking user to change password on logon.
Session timeout	Using this option, you can set default idle session time-out for user in minutes.
Display 'Download SSL Certificate' option, on user's landing page.	Administrator can ask user to download SSL certificate for security purposes.
Display 'Need help/trouble signing in' option, on user's landing page.	Administrator can display help options that the user can use if user is facing difficulty in logging in , for example can display the support website or contact numbers.
Maximum unsuccessful login attempts	Maximum number of allowed attempts to logon after which error message is displayed.
Display Terms & Conditions link to user page.	Administrator can display the legal terms and conditions for using the website. Enter the content as required.
Show copyright to user page.	Administrator can display the copyright notice, legal notices for using the website. Administrator can define the Copyright message that appears.

4. Configure the options as required.
5. Click **Save**. Use the **Reset** button if you want to reset the page.

Branding

The branding feature lets you use your own custom logo on your user logon page. You can upload your product logo, company logo and favicon to suit your requirements. The image file size should be less than or equal to 1 MB.

Notifications

Notifications from the Seqrite UTM inform you immediately about all security relevant events occurring at getaway level, by email or SMS. These events are categorized as error, warning and information.

These notifications are for system-generated events (as specified by administrator). Notifications can be configured to inform about system alerts, hardware status, services status, security, usage and update information.

Notification Medium

You can configure Seqrite UTM to receive notifications for different system events. Seqrite UTM supports the following two types of notifications:

- Email Notification
- SMS Notification
- Alerts

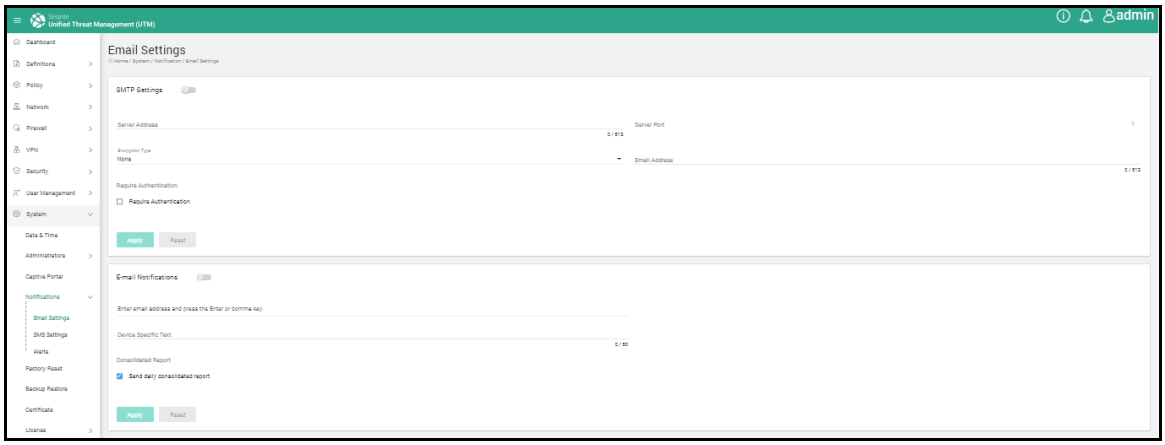
Email Notification (SMTP) Settings

You can configure Seqrite UTM to send you notifications via email for system-generated events. You can configure this using the email notification section. Before configuring the email notifications ensure that you have configured SMTP settings.

The SMTP settings page helps in configuring the email account of the administrator that will be used for receiving email notifications.

Configuring email notifications

1. Navigate to **System > Notification > Email settings**. The Email settings page is displayed:



2. The following table describes the fields on page, configure as required:

Field	Description
Status	Toggle and enable the SMTP status. Email notifications are not sent if status is disabled.
Server Address	Enter SMTP server address. Server address can be a domain name or an IP address.
Server Port	Enter SMTP server port number.
Encryption Type	Select Encryption Type from drop-down list, whether TLS or SSL
Email Address	This is the email address of Admin. All the email notifications will be sent using this email address. Note: This Email address is by default whitelisted for Mail Protection.
Require Authentication	If Require Authentication check box is selected, username and password will be required for SMTP server authentication.

3. Click **Apply** to save the changes.
4. In the Email Notifications section, enter the e-mail addresses that need to be notified.
5. Enter the Device specific text. This can be a short description of the device from which notifications are sent.
6. Select the option for sending consolidated mail report if required. The option is selected by default. If not required, you can uncheck the option. For more information, see Consolidated Report.
7. Click **Apply** to save the configuration.

Consolidated Report

You can configure UTM to send you a consolidated report in HTML format at the end of the day that contains the following information:

- Status of Bypass Security Policies feature
- System information: CPU usage, Model, version, Product Key, Expiry date, System up time and Boot time
- Security information about viruses detected, policy breaches, intrusions detected and signature updates
- Bandwidth utilization graph for present interfaces with upload, download statistics
- Average interface data usage statistics
- Top User list by data usage
- WAN interface usage hourly usage report for upload and download usage.

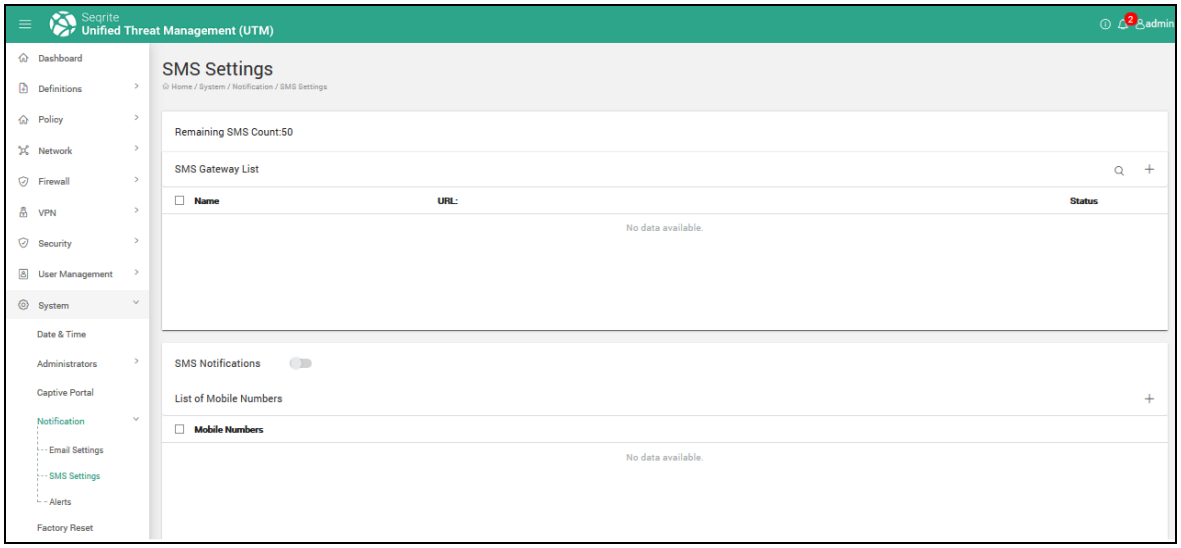
SMS notification settings

You can configure Seqrite UTM to send SMS or you can add SMS Gateways to send notification SMS for system-generated events and guest user authentication. To configure Seqrite UTM to send SMS notifications, follow the steps given below:

Note: To set Seqrite UTM's SMS gateway and enable the SMS Notification feature in your Seqrite UTM, you need to contact the Seqrite UTM Support Team.

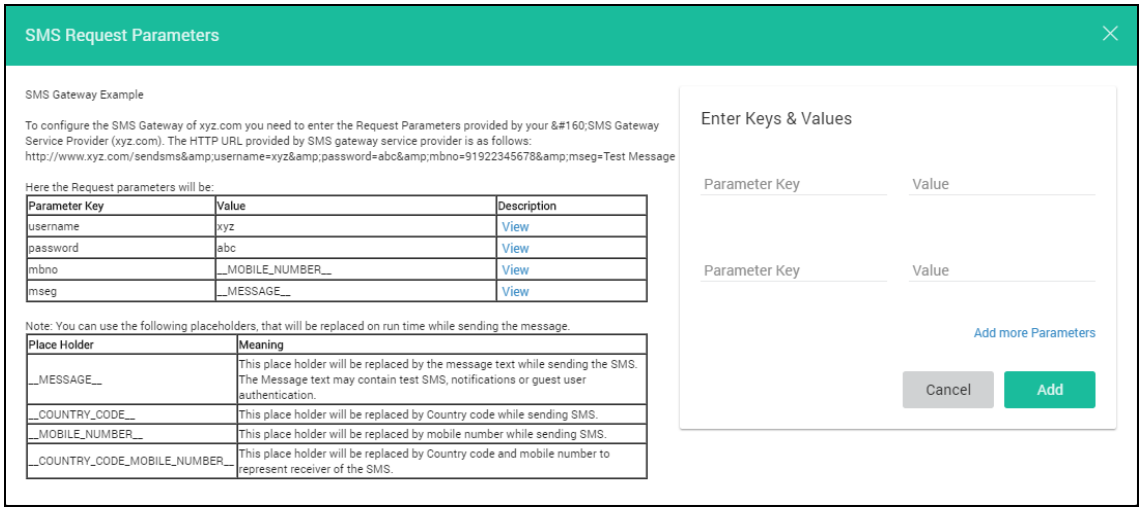
Adding SMS gateway

1. Navigate to **System > Notifications > SMS Settings**. The SMS notifications configuration page is displayed.



Note: The **Remaining SMS** count displays the total number of SMS notifications that can be sent from the Seqrite UTM. These SMS count are displayed only for the Default SMS Gateway.

2. In the SMS Settings area, Click the **+(Add)** icon to add the SMS Gateway.
3. Enter the name, URL, select the HTTP method, and if required enable logging of SMS Gateway response.
4. In the Request Parameters section, click **+ (Add)** to add the SMS request parameters, then enter the parameters as required.



Note: The parameters are provided by your Service Provider to configure the SMS Gateway.

You can use the following placeholders that will be replaced on run time while sending the message. To configure third party SMS Gateway in Seqrite UTM, the following 2 placeholders are required and must be added under the Request Parameter:__MOBILE_NUMBER__ and __MESSAGE__.

5. Click **Add** and then, click **Apply**.
6. Click **Test SMS** button, to send a test message to check if the SMS gateway is configured.
7. Click **Save**.

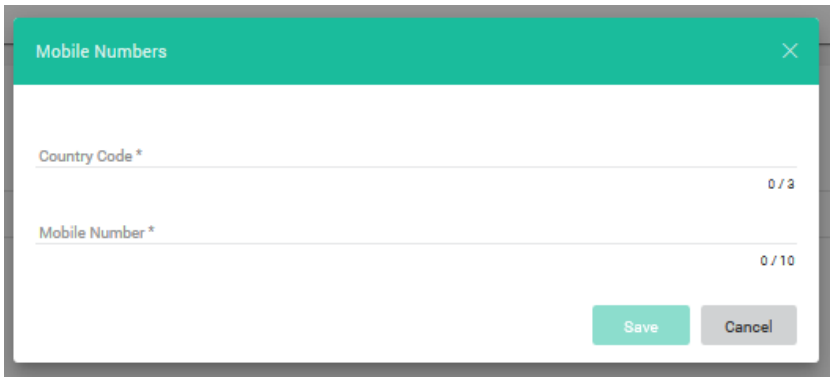
Edit SMS Gateway

1. Navigate to **System > Notifications > SMS Settings**. The SMS notifications configuration page is displayed.
2. In the SMS Gateway Settings section click on the SMS gateway name.

   The SMS Gateway edit page is displayed.
3. Make the required changes and click **Save**.

Enabling SMS Notifications

1. Navigate to **System > Notifications> SMS Settings**. In the SMS Notifications area, toggle the SMS Notifications switch to enable SMS notifications.
2. Click **+ (Add)** to add mobile numbers.



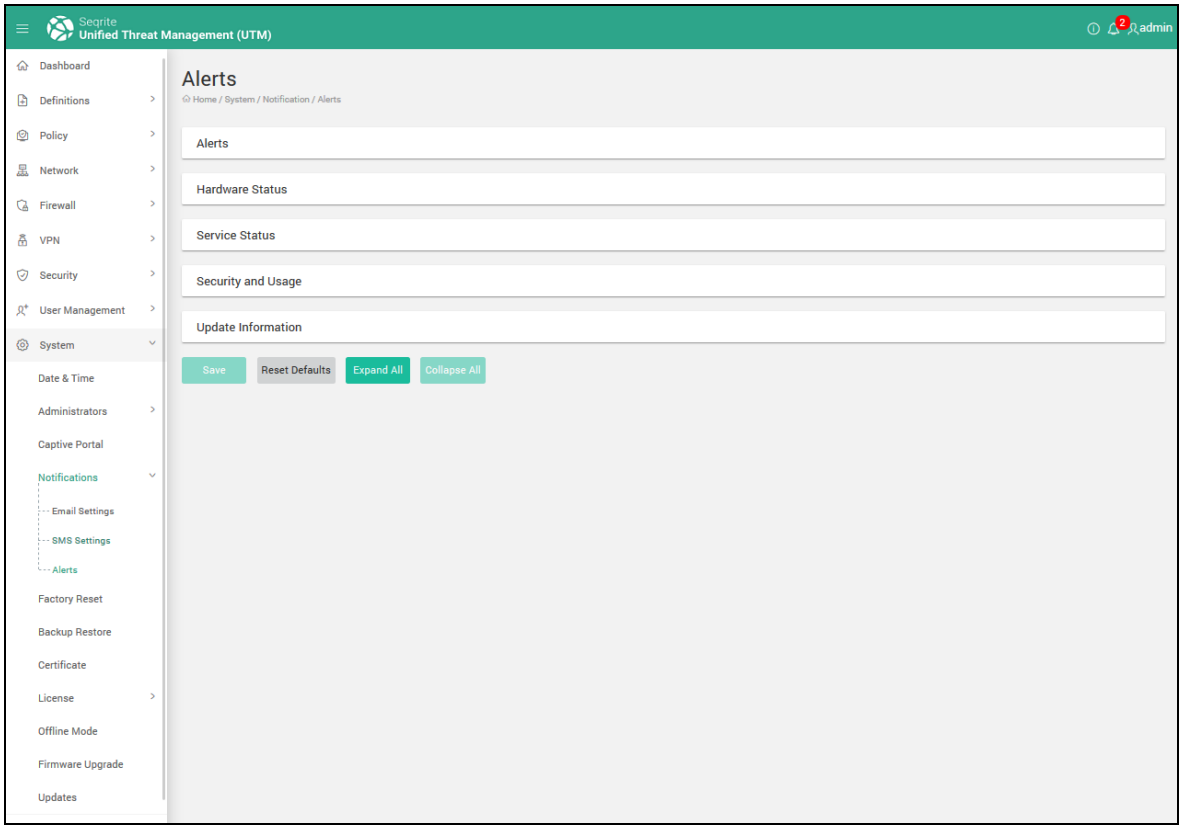
3. Enter the Country code and the mobile number.
4. Click **Save**. The mobile number is added to the list of mobile numbers to whom the SMS notifications will be sent.

Configuring Alert notifications

You can configure which notification type, either email or SMS should be sent on an event or alert related to system, hardware status, services status, security, usage and update information.

System

1. Navigate to **System > Notifications > Alerts**. The Alerts configuration page is displayed.



2. Click on the tabs to expand and view the events. Select Email or SMS notification type for respective events. The different notification types are explained below:

   Alerts: These are Seqrite UTM alerts or critical situations for which an administrator gets notifications. For e.g. If administrator has configured e-mail and SMS notifications for 'Antivirus protection is out of date', then administration will receive e-mail and SMS when the antivirus protection has expired.

   Hardware Status: Administrator receives notifications for hardware status. If CPU usage reaches 90%, a notification is sent. If disk usage reaches 85%, notification is sent.

   Service Status: If crucial services stop their execution, which hampers security of the network then administrator gets notification. Service are mainly HTTP proxy service, content filtering service, antivirus service, IPS service and mail protection service.

   Security and Usage: If the security of the network is hampered or of the Internet usage is greater than the set value, administrator gets notification. These are mainly total Internet usage, total viruses blocked, total Intrusions prevented and Mail protection statistics.

   Update information: Notifications related to IPS, Antivirus and Seqrite UTM product update are sent.

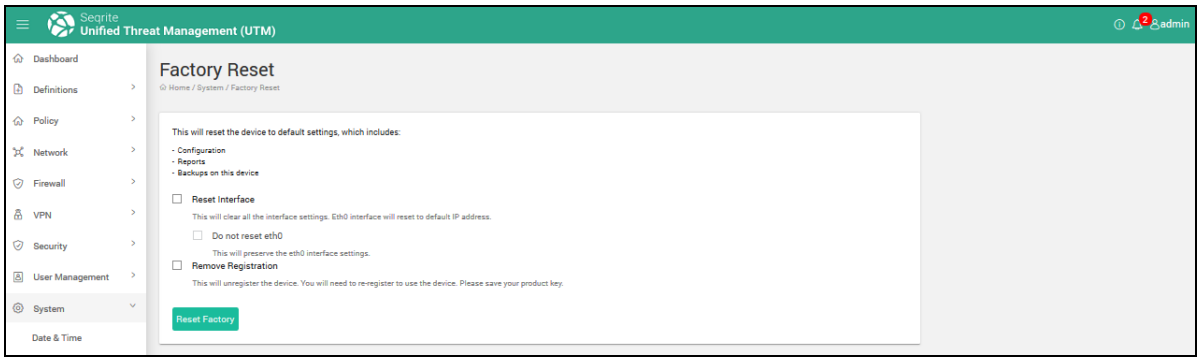
3. You can click on **Expand All** link to view events under all tabs.

4. After selecting the notification type, click **Save**.
5. You can also click the **Reset Default** link to set the notification configuration as per default setting.

Factory reset

With the factory reset, the Seqrite UTM can be rolled back to the original state in which it was shipped. You have an option to reset the interface and also remove the registration. If you choose to select Factory Reset, all Seqrite UTM Settings, User Defined Settings, and reports will be lost.

1. Navigate to **System > Factory Reset**. The Factory reset screen is displayed.



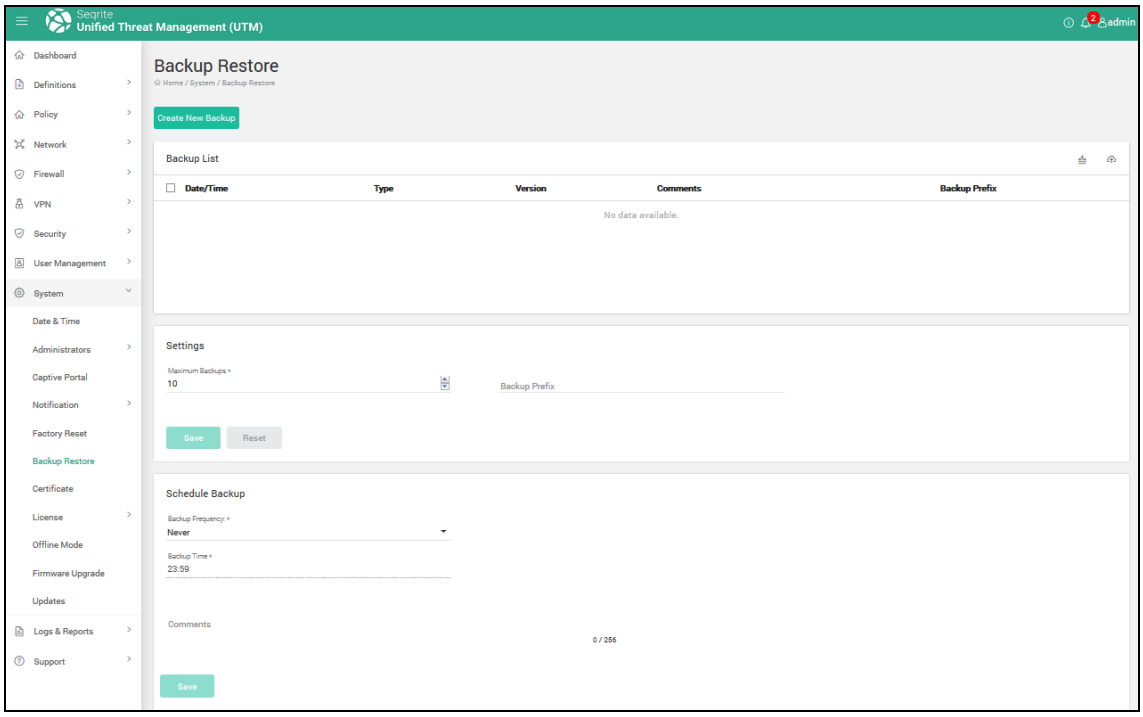
2. Select the option to reset Interface of you want to reset the Interface settings. This will cause the loss of all IP address, gateway, and will reset to default IP address.
3. If you want to preserve the eth0 settings even if a reset is performed, place a check mark against the option *Do not reset eth0.*
4. Select the Remove Registration option if you want to remove the registration. You need to register Seqrite UTM again in order to use it.
5. Click **Factory Reset**. The Seqrite UTM appliance is reset to factory defaults and will have to be configured again.

Backup and Restore

Seqrite UTM allows to take backup of the settings, configuration and data which can help in case the Seqrite UTM crashes or if you want to revert to the previous settings. You can take backup of Seqrite UTM default settings, user defined settings, and user database settings and store it to reuse in case of any technical emergency. You can also schedule the configuration backup to be sent automatically to your email address when backup is taken manually or scheduled for a later date and time.

Creating a new backup

1. Navigate to **System > Backup and Restore**. The Backup and Restore settings page is displayed.



2. Click **Create a new backup**.
3. Add comments if any that are required.
4. Select the option to send backup file over email if required. Note: You must carry out the following under **System > Notifications > Email settings** before you can use this feature.
    - Enable the UTM Backup option.
    - Configure the email notifications settings under SMTP settings and enable the UTM Backup in relevant section.
5. Click **Backup Now**. The data is backed up and displayed in the list of Backups with the timestamp and version number.

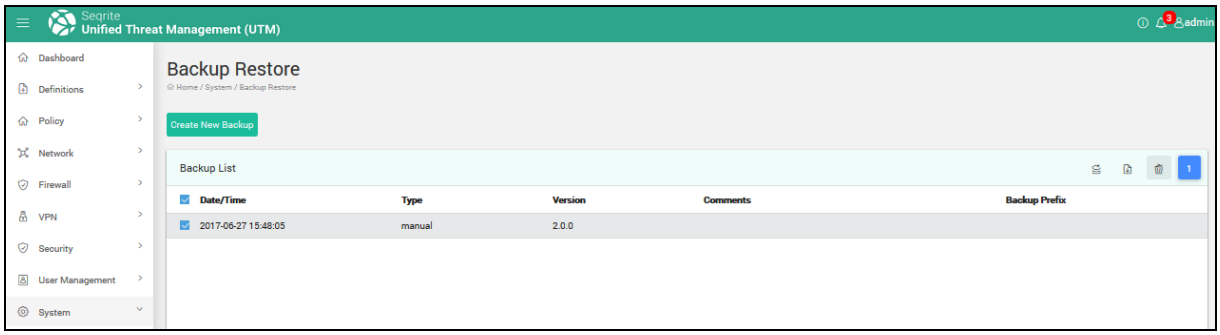
Scheduling Automatic Backup

This feature allows you to schedule the Seqrite UTM to take automatic backup of the system configurations on a scheduled time. This backup is stored on device and can be used to restore the system configurations whenever required.

Note: Automatic Backup does not contain reports and other data of the system.

1. Navigate to **System > Backup Restore**.

2. In the Schedule backup section, select the frequency of backups, date and the Backup time.
3. To exclude the backup of certificates and emails, select the corresponding options.
4. Click **Save.**



Note: The Backup page also displays a list of all previously taken backups with the time and date and the type of backup taken, whether it is configuration or data backup. You can download the backup files by clicking on the backup file link in the Configuration Backup / Data Backup column.

Using the Import option

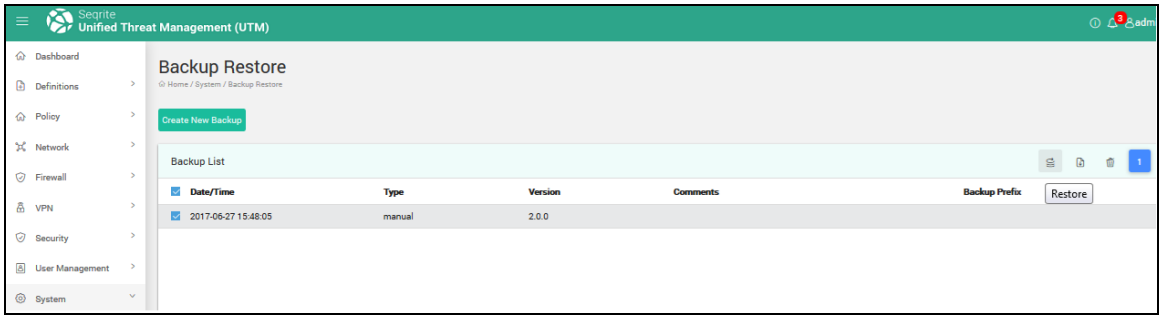
You can also import backups from the disk or another location and restore it.

1. Navigate to **System > Backup Restore**.
2. In the Backup Restore section, click the Import icon on the upper right corner to browse and import the backup file.
3. Click **Upload File**.
   Note: The file must be of the .bak extension.

Restoring a backup

This feature allows you to rebuild the damaged data from the backup taken previously. The backup of all the configuration and reports is stored on the Seqrite UTM. You can also upload data from local machine to Seqrite UTM.

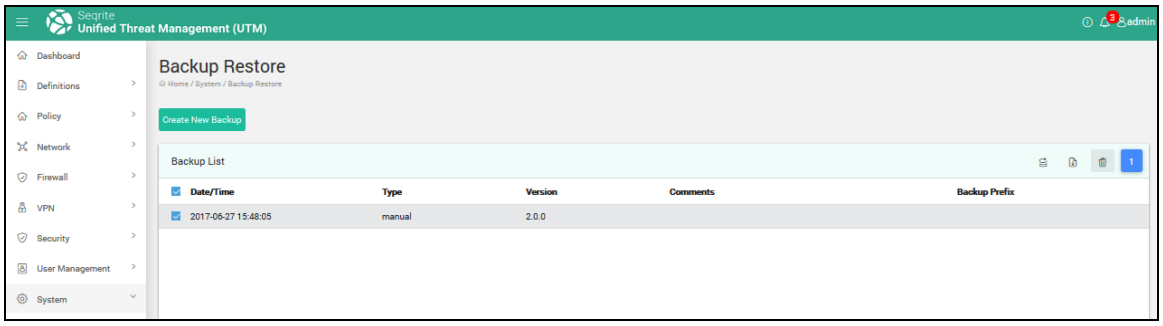
1. Navigate to **System > Backup and Restore**. The Backup and Restore settings page is displayed with a list of all previously taken backups with the time, date and the type of backup.



2. From the Backup list, select the backup you want to restore.
3. Click the **Restore** icon. The backup will be restored.

Deleting a backup

1. Navigate to **System > Backup and Restore**.



2. Select the backup you want to delete and click the **Delete** icon. Click **Yes** in the Delete confirmation box. The selected backup is deleted.

Scheduling a backup

1. Navigate to **System > Backup Restore**.
2. In the Schedule Backup settings section, select the frequency from Never, Monthly, Weekly, or Daily.
3. Select the date and time for the scheduled backup.
4. Enter special comments if any.
5. Select the options to exclude certificates and emails as required.
6. Click Save.

Setting maximum number of backups

1. Navigate to **System > Backup Restore**.
2. In the Settings area, specify the maximum number of backups to take.
3. Enter the backup prefix if any.
4. Click **Save**. The Seqrite UTM will backup only as per the schedule and the maximum number of backups specified. The backups are refreshed in the backup list.

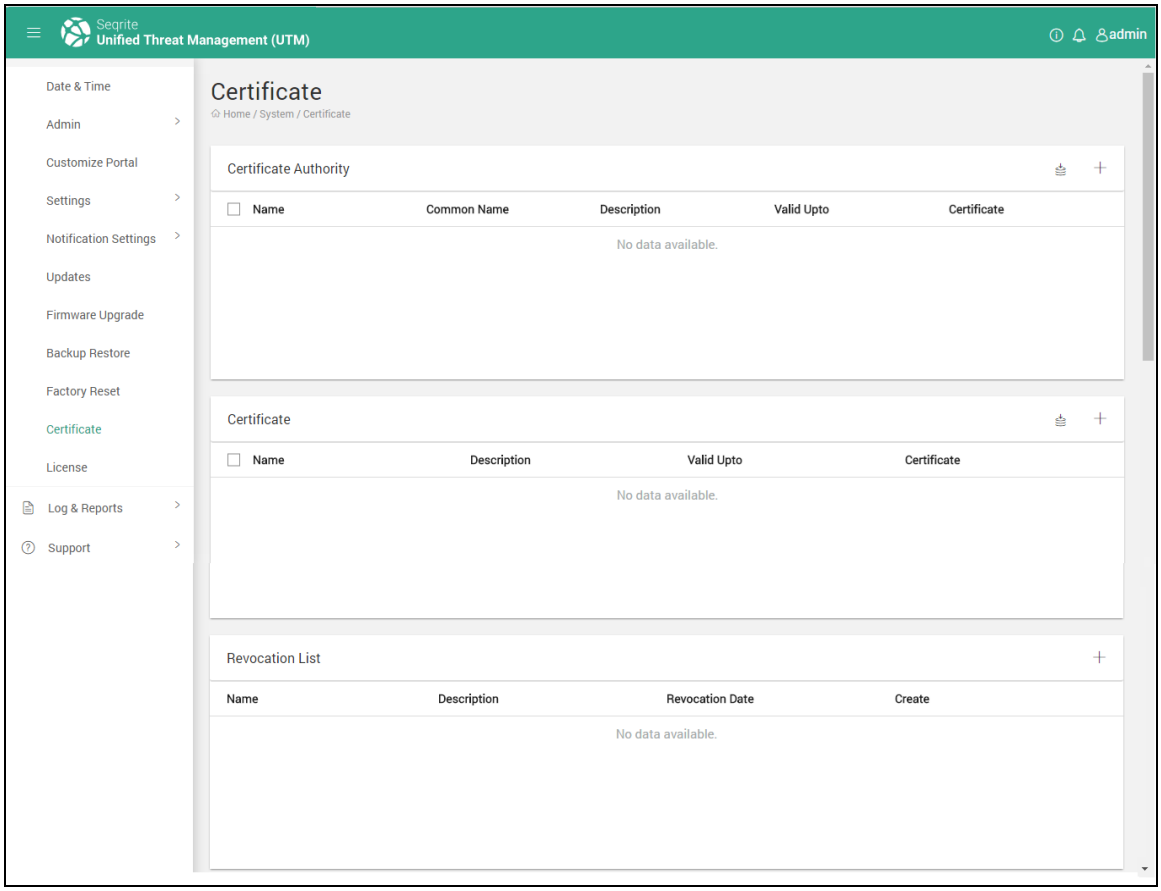
Certificates

A Certificate is an attachment to an electronic message used for security purposes. The most common use of a certificate is to verify that a user sending a message is legitimate, and also provide the receiver with the means to encode a reply. You can either add self-signed signatures or import certificates signed by third party Certificate Authority (CA). A certificate authority (CA) is an authority that issues and manages security credentials and public keys for message encryption.

Seqrite UTM allows you to manage the Certificate Authorities, certificates, create self-signed certificates that can be used for authentication while launching a VPN connection. You can also import, third party certificates and download the Certificate Authorities and Certificates. Seqrite UTM helps you to maintain a revocation list of certificates.

Managing certificates

1. Navigate to **System > Certificates.** The following page is displayed.



The page is divided in the following three sections:

- Certificate Authority
- Certificates
- Revocation list

2. To add Certificate Authority / certificates, click the + (**Add)** icon in the respective section. The **Add Certificate** dialog box is displayed.
3. Enter the details such as Name, Common Name, select CA, Country, State, Locality name, Valid Up to date, Email, then click **Save**.

   Note: While adding Certificate, you need to select the associated CA.
   Space is not allowed in Name and Common Name.
4. You can import third party certificates and Certificate Authorities. To import certificate / Certificate Authority click **Import** in the respective section, enter the Name and password, select the appropriate option for import as file type, provide relevant description, click Browse, choose a file, and click **Ok**.

   Note: For importing Certificate Authority PKCS12, PEM, DER file format is allowed. If you select PEM or DER file format, then you will get an option to import Private key, which is optional. This key will be required when the imported CA is used for signing certificates.

   - For importing Certificate only PKCS12 file format is allowed.
5. The SSL VPN **Revocation List** displays the list of blacklisted connections, description and the date they were added to the revocation list. This option can be utilized to stop connections in case the certificate is lost or stolen. To revoke / block a client certificate click **Add** in the revocation list section. Select the **Connection name** from the list of existing connections.
6. Click **Save**.

License Details

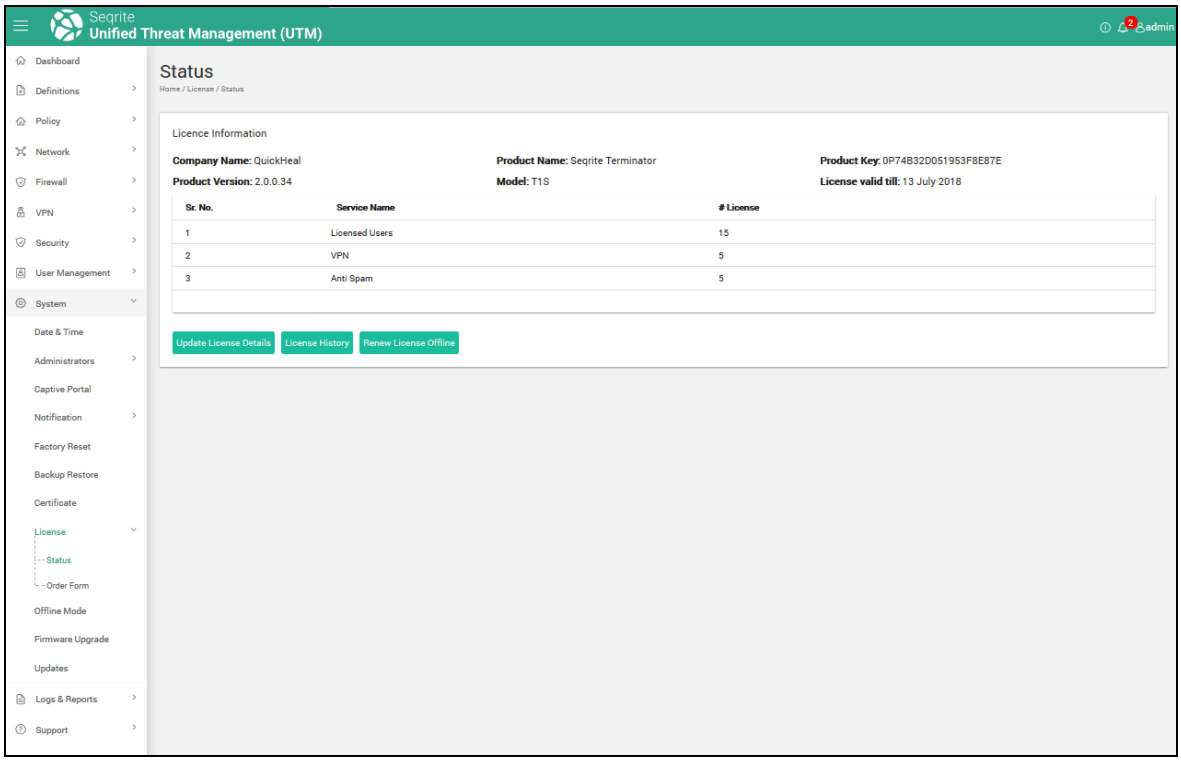
The License Details page displays the license information about the Seqrite UTM. It includes the following details:

- **License details**: This includes the company name, product name, product key, product version, model and license expiry date.
- **Service details**: This includes the services that you have opted for, such as number of licenses, number of VPNs, antispam and Seqrite cloud service.

Using the license details page you can update license details, view license history, renew license online as well as offline and also activate Seqrite cloud service.

Viewing license details

1. Navigate to **System** > **License > Status.** The License Details page is displayed.



The following table explains the fields in the License Information section:

Company Name	Displays your company name.
Product name	Displays the product name.
Product key	Displays product key.
Product Version	Displays the version of Seqrite UTM.
Model	Displays the model type of the Seqrite UTM.
License valid till	Displays the date until which the license is valid. After this date the License will expire, and you need to renew the license.

2. The service Name section displays the details of the services you have opted for. For e.g. if you have bought the Antispam service, then it will be displayed in this section. Click **Update the License details** to get latest updates from the server if some information has changed.
3. To view the license activity details such as renewal, addition or removal of services, click the **License History** button. The license history popup is displayed.
4. To renew license offline in case of there is no internet connection, click the Renew License offline button. The renew license offline popup is displayed. Follow the steps given in the popup to renew license offline.

Placing an order for License/Features

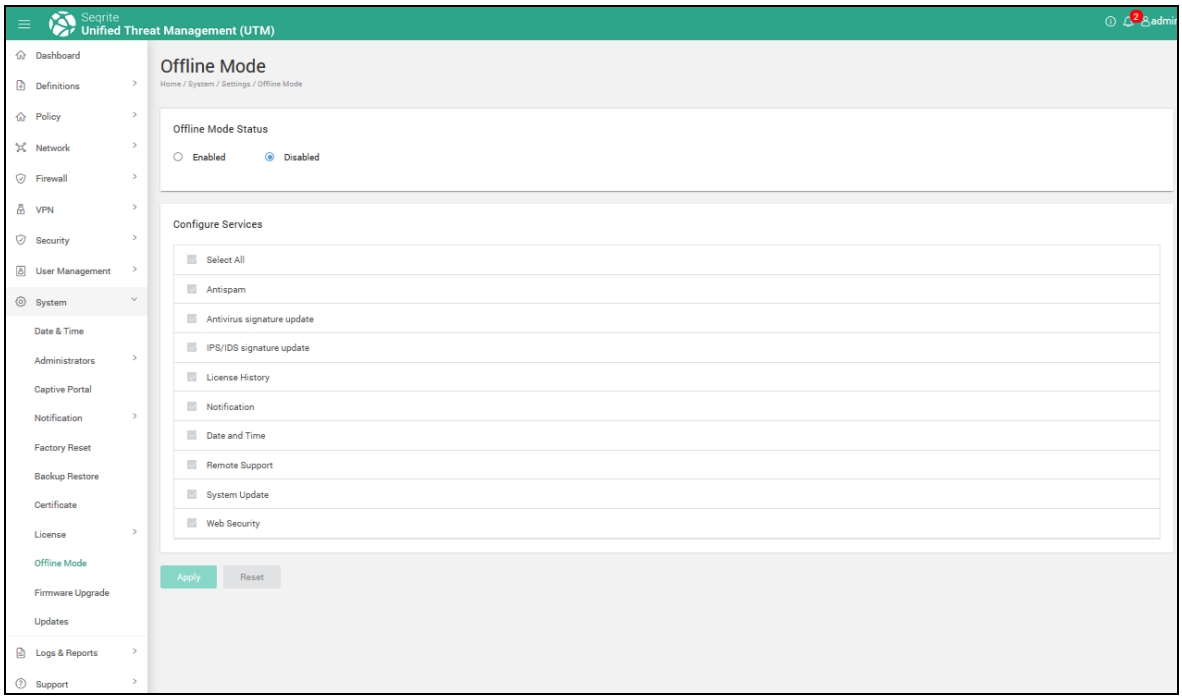
You can renew the Seqrite UTM license as well as add more users for the license using the Order form tab on the License details page.

1. Navigate to **System > License > Order Form**. The License Order page is displayed.
    a. To renew license, select Renew my license
    b. To buy additional features, select the option Buy additional features
2. Click **Place an Order**. The product key is validated and the browser redirects to the Seqrite Web site.

Configuring the Offline mode

To stop services from using the Internet, you can select the Device offline mode. You can also select the services that can be set as offline, using the **Configure Services** button. The following services are available in the Offline mode:
Antivirus Signature update, IPS/IDS Signature update, License History, Notification, Date & time, Remote Support, System Update, and Web Security.

1. Navigate to **System > Offline mode.** The following page is displayed.



2. Enable **Offline** mode, a list of services displayed.
3. Select the services that you want to be offline and click **Apply**.

Note: These services will be offline only if the **Offline** mode is selected.

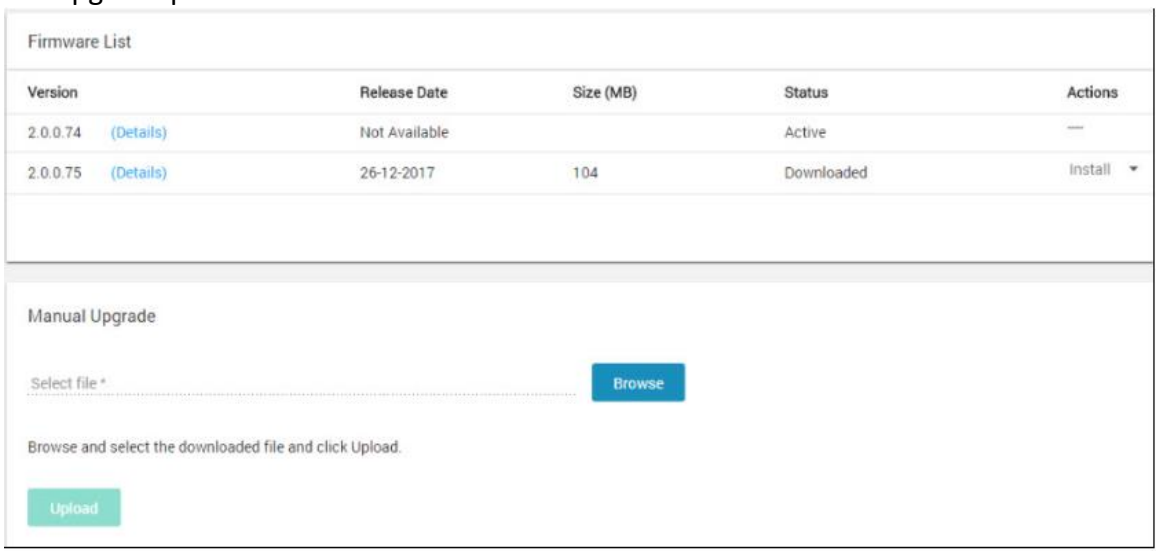
Firmware Upgrades

This section lists the latest firmware versions that may be available for upgrade. You can use this information to upgrade your UTM firmware to the latest firmware version. For e.g. from 2.1x.x to 2.2x.x

Note: This is a major process and involves downtime, it also has to be performed manually.

1. Navigate to **System > Firmware Upgrade**. The list of firmware with details is displayed.

2. Click on **Details** to view the details of changes.
3. Depending on your requirement, you can select the options from the Actions List. You can download and install immediately or, only download the file and install later or download later.
4. If you have downloaded the upgrade file, the list of firmware displays the details as downloaded. In the Actions drop-down, the install action is then available for you to carry out the upgrade process.

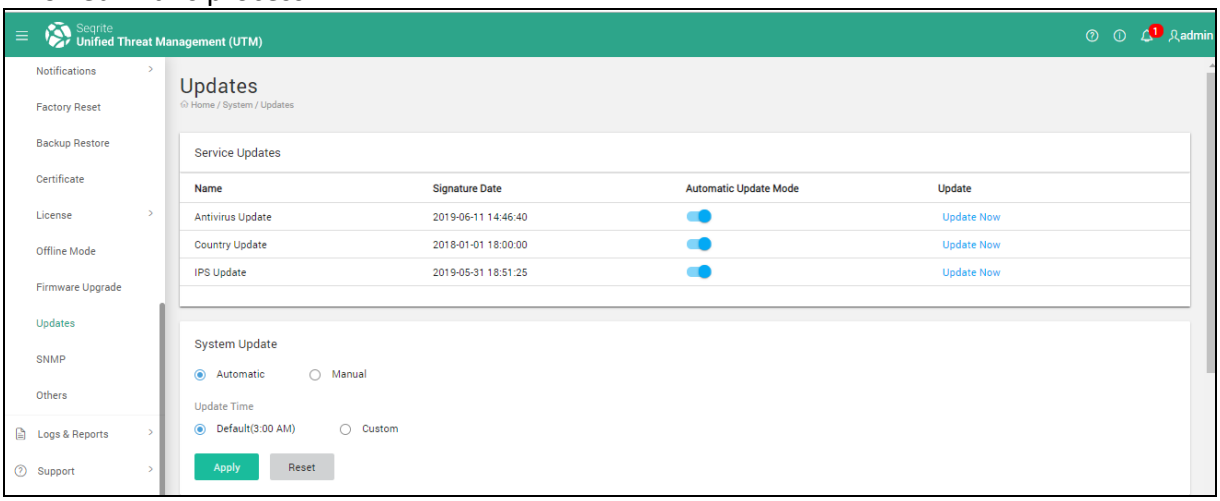


5. If you have the upgrade file manually copied on your computer, you can browse and upload the file for installation. To do so, in the Manual Upgrade section, click **Browse**, navigate to the upgrade file, and click **Upload**. Note: A file with .enc extension is used for upgrade.

6. After the upload process is over, the upgrade details are listed in the Firmware list. In the Actions list for that entry, Install Now and Install Later options are displayed. You can choose any of the options for installation as per your requirement.

Obtaining Service and System Updates

You can manage the Seqrite UTM service and system updates using the Updates page. The Service updates include Antivirus and IPS/IDS signature updates, and the Country Update for country based-based blocking whereas system updates include the stability / bug fixes.
Note: Applying the Service and System Updates is a minor process and there is not downtime involved in this process.



Configuring Service Updates

1. Navigate to **System > Updates.** The Service Update details are displayed.
2. Set the Service updates to be applied automatically or manually by toggling the Automatic Update Mode button.
    - Automatic update: If enabled, the updates are applied automatically at the specified time.
    - Manual (Automatic Update mode disabled): If set to manual, updates are not applied unless the admin clicks Apply.
3. Click **Update Now** to install the available updates for the particular service.

Configuring System Updates (Patches)

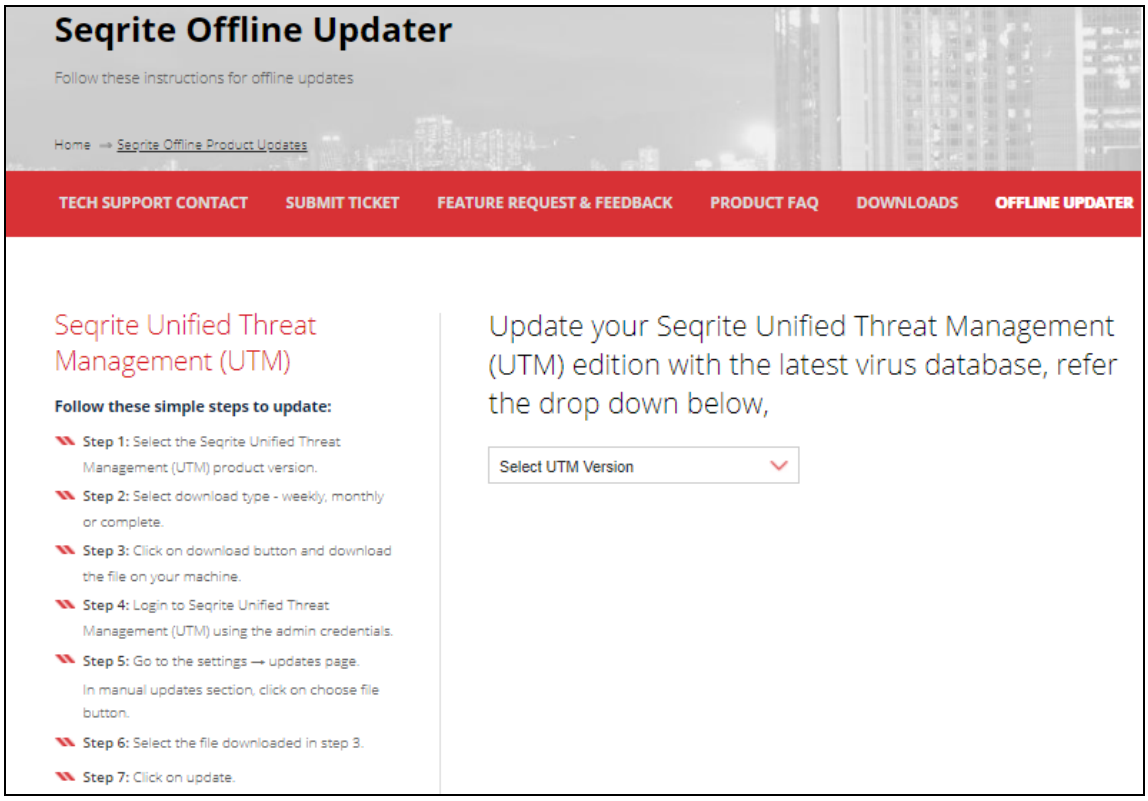
1. Navigate to **System > Updates.**
   In the System Update section, select whether you want the System updates to be carried out Automatically or Manually by selecting the appropriate option.
2. Select the update time, whether default (at 3.00 AM) or customized, enter applicable time and click **Apply**.

Performing a manual update

You can perform service and system updates manually also if required and when updates are available. You must first copy the updates to your system.

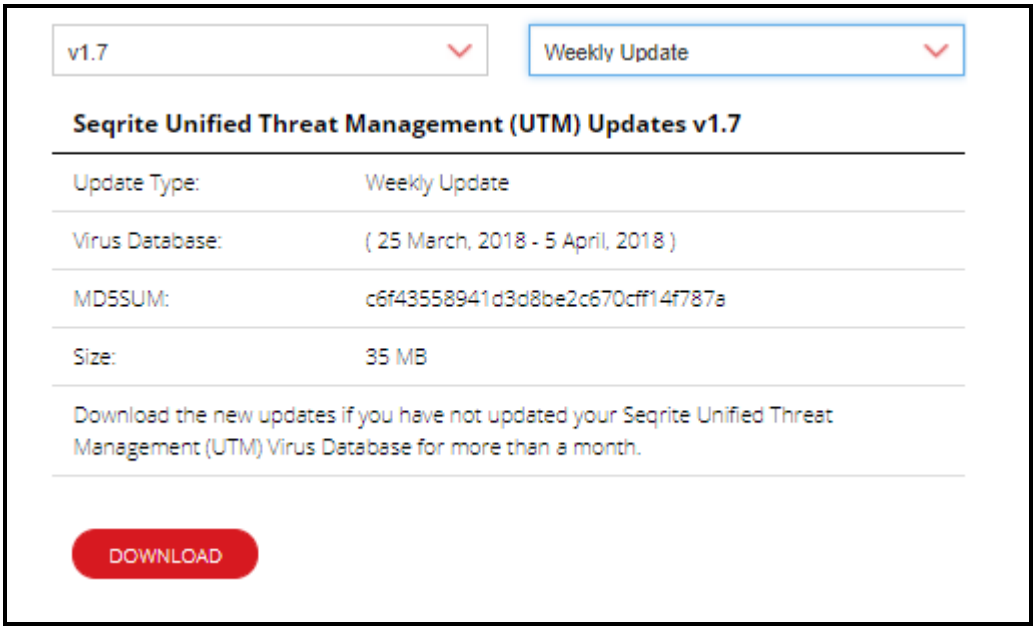
1. Navigate to **System > Updates**. In the Manual Update section to download the Update file, click on the *Click here* link. You can also paste the following link in your browser.

   http://www.seqrite.com/seqrite-offline-product-updates.
   Note: For downloading you must have an active internet connection. The Seqrite Offline Update site is displayed.



2. Click on the Seqrite UTM tab.
3. Select the Seqrite UTM Version.

4. Select the type of update from weekly, monthly and complete. This depends on the last updates taken.



5. Click **Download**. The update file with the .tar extension is downloaded on your computer.
6. In the Manual Updates section on the same page, click **Browse** and choose the file and click **Update**.
   Note: The file extension should not be changed. In case of insufficient space on device, extract the update files and upload individually.
7. Wait till the update process is completed. After the manual update process is completed a message is displayed, informing if the manual update was successful or failed. You can also go to **Logs & Reports > Log Viewer > Updates** and confirm.

SNMP

The Simple Network Management Protocol (SNMP) manager lets you monitor event-driven alerts and operational statistics for the UTM. The statistics that are obtained along with the traps can help track resource limitations, system changes and failures.

You can send GET requests from your SNMP manager and in response configure alerts by forwarding log data as traps and enable the delivery of statistics. Each trap and statistic have a unique object identifier (OID).

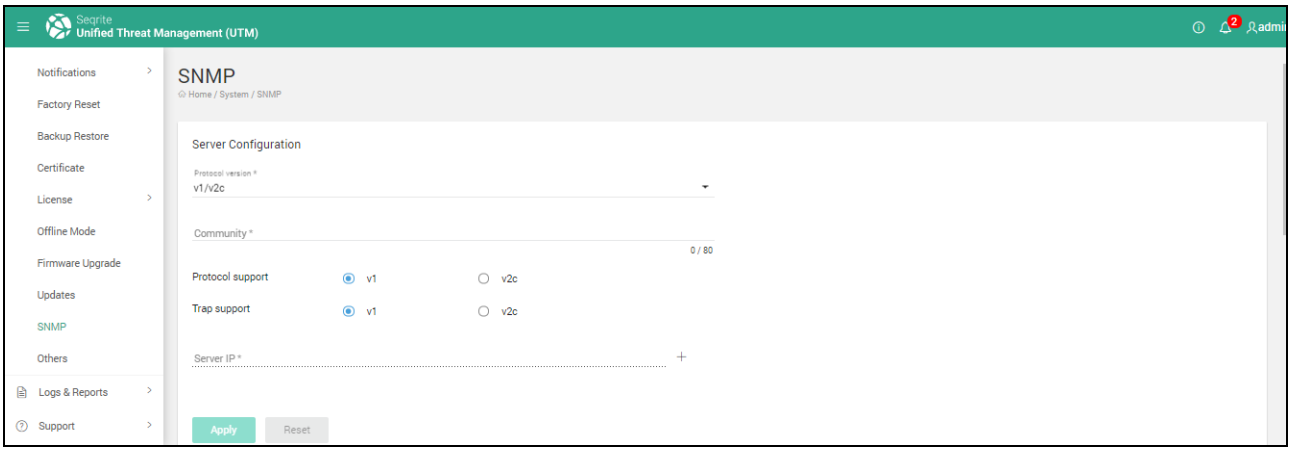
The SNMP manager uses MIB files from each agent to decode the OIDs (strings of numbers) and translate them into meaningful information. When an event triggers SNMP trap generation (for example, an interface goes down), UTM responds immediately by updating the corresponding SNMP object (for example, the interfaces MIB). This ensures that the configured SNMP manager displays the latest information when polling an object to confirm an event.

UTM supports SNMP Version v1, v2c and v3. You can use the version based on the devices in your network and on your network security requirements. SNMPv3 is more secure and enables more granular access control for system statistics than SNMPv2c.

To use SNMP for monitoring UTM, you must first load the Supported MIBs into your SNMP manager. Next you need to determine which object identifiers (OIDs) correspond to the system statistics and the specific traps you want to monitor.

Configuring SNMP server details

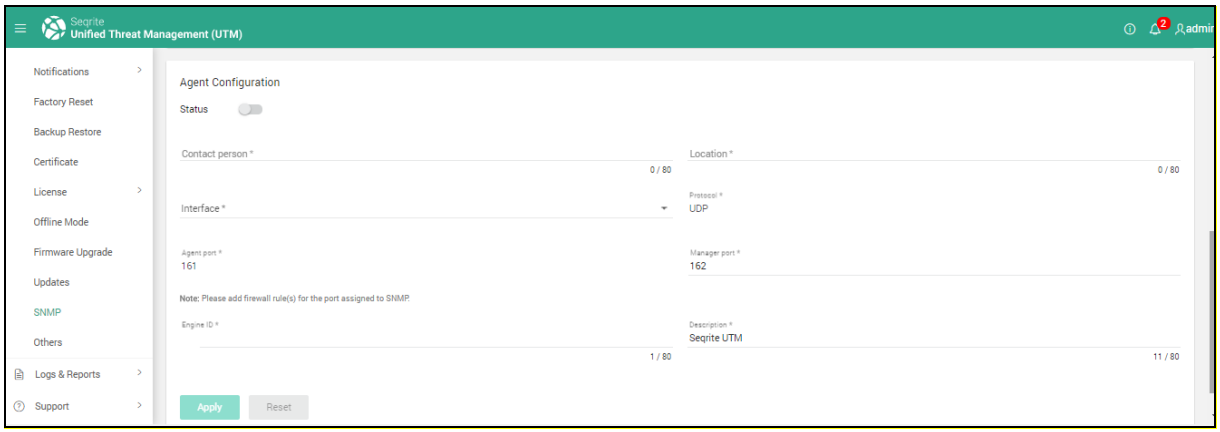
1. Navigate to **System > SNMP**.



2. Select the protocol version from the drop-down list. You can either select a combination of v1/v2C or v3.
    a. If you select v1/v2C option, enter the community name. and select the protocol and trap versions and IP address as required.
    b. If you select the v3 option, enter the Username, IP address. Next select the authentication type. Based on the authentication type selected, configure further options such as authentication protocols, Privacy protocols and the corresponding passwords.
3. Click **Apply**.
   Note: If you select v1/v2C, protocol and trap support v2C is recommended, and if you select v3, Authentication with SHA and privacy with AES is recommended.

Configuring the Agent details

1. Navigate to System > SNMP.



2. In the Agent configuration area, enable the agent service by toggling the status button.
3. Enter the contact person details such as name and location.
4. Select the interface through which the agent will communicate with the SNMP server.
5. Under **User Management > Users**, create a new user as SNMP Manager and add the IP address of the SNMP manager.
6. Ensure that the agent port number 161 (For Get requests) and the Manager port numbers 162 (For traps) are configured in the Interzone Firewall rules. See the following examples:
   - If the SNMP manager is configured in the WAN zone of the UTM then the firewall rule must be configured as:

     ALLOW 161 FROM WAN to UTM (For GET requests)
     ALLOW 162 FROM UTM to WAN (For traps).
   - If the SNMP manager is in the LAN zone of UTM, the firewall rule must be configured as follows:

     ALLOW PORT 161(SNMP) from LAN to UTM. (FOR SNMP Notifications).
     ALLOW PORT 162(TRAPS) from UTM to LAN. (FOR SNMP traps)
   - If the SNMP manager is in the BRIDGE zone of UTM, the firewall rule must be configured as follows:

     ALLOW PORT 161(SNMP) from BRIDGE to UTM. (FOR SNMP notifications).
     ALLOW PORT 162(TRAPS) from UTM to BRIDGE. (FOR SNMP traps)
7. Enter the Engine ID and the relevant description.
8. Click **Apply**.

Others

Changing the host name

You can change the host name for your UTM appliance as required.

1. Navigate to **System > Others**.
2. Enter/Modify the host name as required. (The name must be a fully qualified domain name.)
3. Click **Save**.

Diagnostics and Usage

Use the toggle switch to enable or disable Diagnostics and Usage option.

Changing the product key

1. Navigate to **System > Others**.
2. Click **Change Product Key**. The Registration wizard is initiated, and the License agreement screen is displayed.
3. Follow the registration process as outlined for the Registering the product (Online) wizard.

Chapter 13

Logs and Reports

Seqrite UTM provides extensive reports and logs for various modules. These reports and logs are very useful for troubleshooting and you can take decisions and formulate official policies with the help of the reports. You can get detailed reports on Internet Usage, Web site Access, Mail Protection, etc. You can also export all these reports to .XLS, .PDF or .DOC format for further use.

Reports

The following categories of reports are available on Seqrite UTM:

- Internet Traffic
- Security Protection
- Updates
- Logs
- Settings

Internet Traffic

The following types of Internet traffic reports are available on Seqrite UTM:

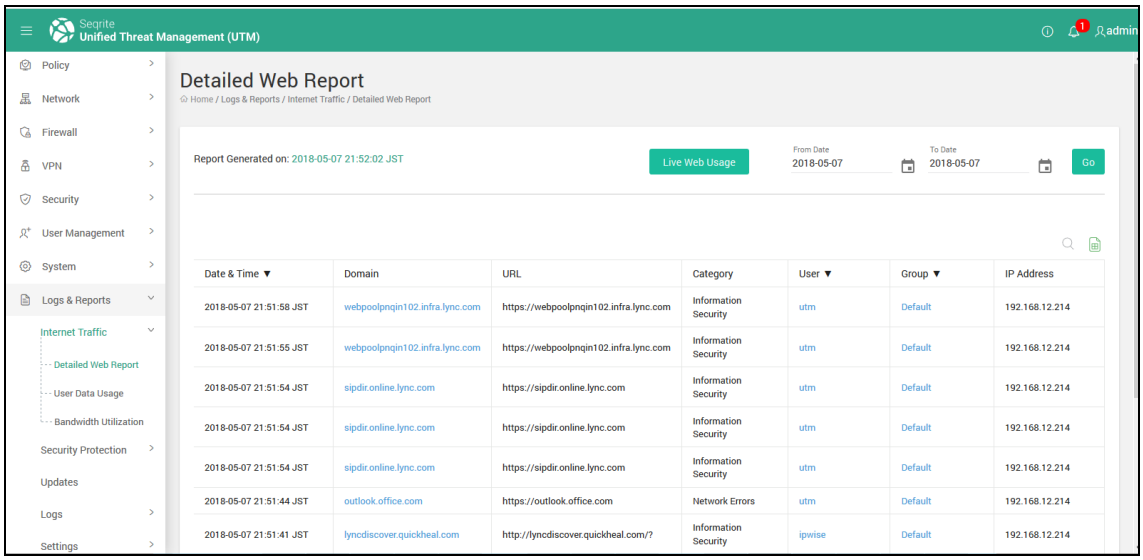
- Detailed Web report
- Live Usage
- User Data Usage Report
- Bandwidth Utilization

Viewing Detailed Web Report

This report displays the information about the Web sites accessed by the users for a particular day or a particular date range. It also displays the date and time of access, domain, URL, category, User, Group, and IP address of the accessing user. You can export this report in the MS Excel, PDF

and MS Word format.
Note: If host is behind router than Mac address of router will display in reports.

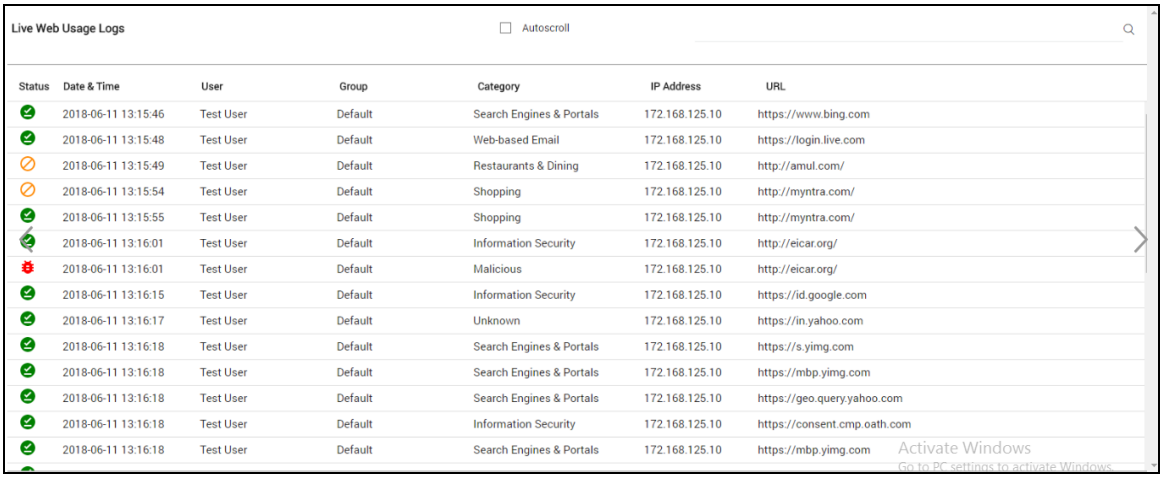
1. Navigate to **Logs and Reports > Internet Traffic > Detailed Web Reports**.
2. Enter the date range for the duration you want the reports.
3. Click **Go**. The report for the selected duration is displayed. You can export this report in the MS Excel, PDF and MS Word format.



Viewing Live Web Usage logs

You can view the real-time web surfing logs for the all the active users (Named and IP-wise users) on UTM containing User IP, User Name, URL Category & URL access status.

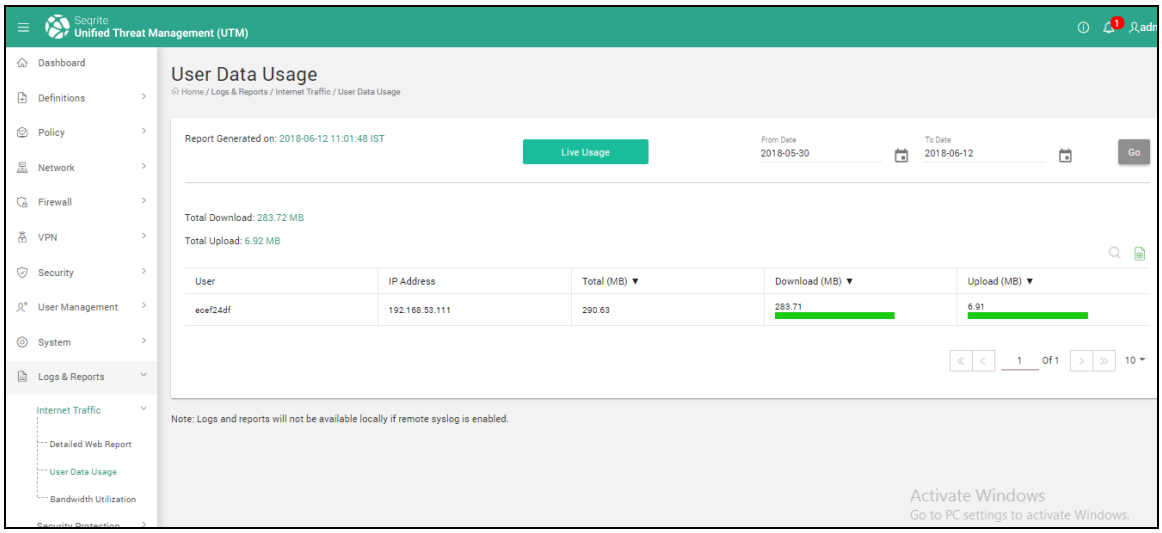
1. Navigate to **Logs and Reports > Internet Traffic > Detailed Web Usage**. The Web usage page is displayed.
2. Click **Live Web Usage**. The live usage report is displayed in a separate browser window.



User data usage

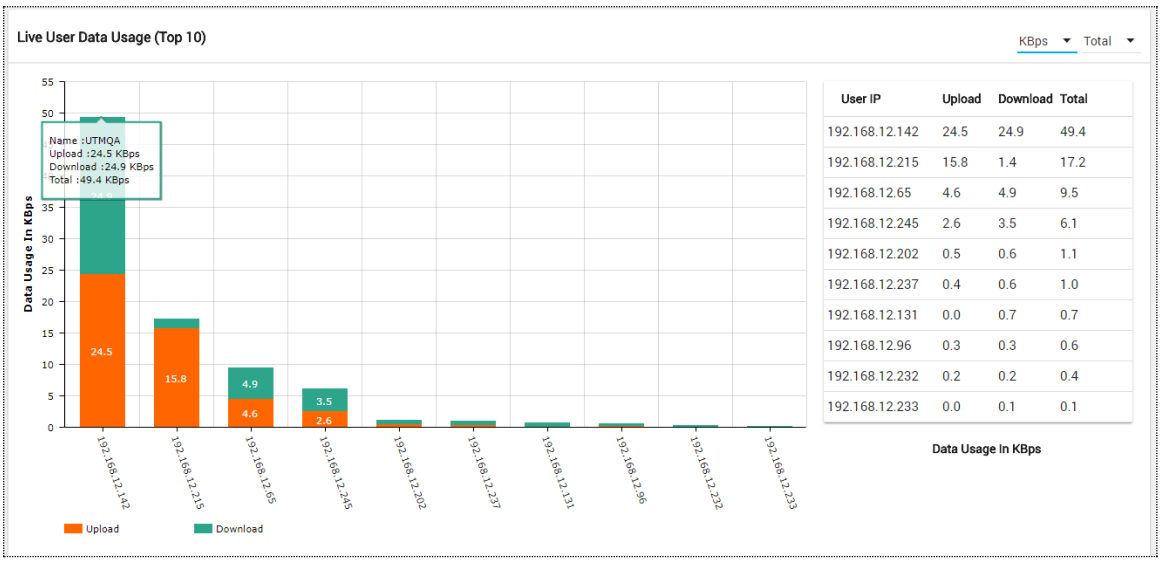
The User Data usage report provides the information about the Internet usage with name of the user, IP address, usage in MB, download and upload usage in MB. This report is available for the last 30 days.

1. Navigate to **Logs and Reports > Internet Traffic**.
2. Click **User Data Usage**. Enter the duration for which you want to view the reports.
3. Click **Go**. The reports for the selected duration are displayed.



Viewing the Live Usage

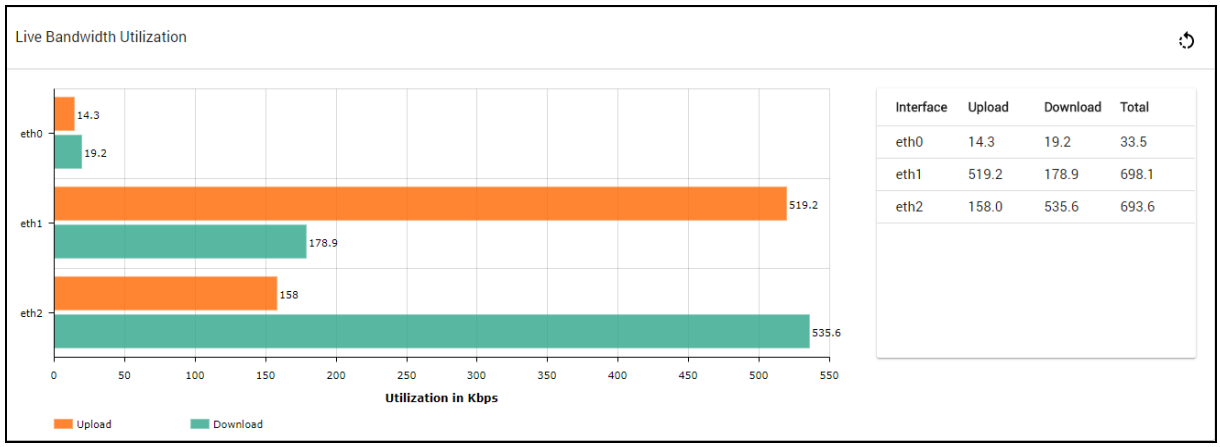
The Live usage graph displays top ten users according to the data usage. This graph displays data usage of all kinds of users Named, IP-wise and direct user. There is an option to view the data usage in terms of KBps (kilo Byptes per second) or MBps (Mega Bytes per second). Each bar of diagram represents data usage of a particular IP Address in terms of upload and Download. Hover the mouse on each bar to display the user details. The page refreshes at every 5 secs and displays 'No data available' if there is no current data usage by anyone.



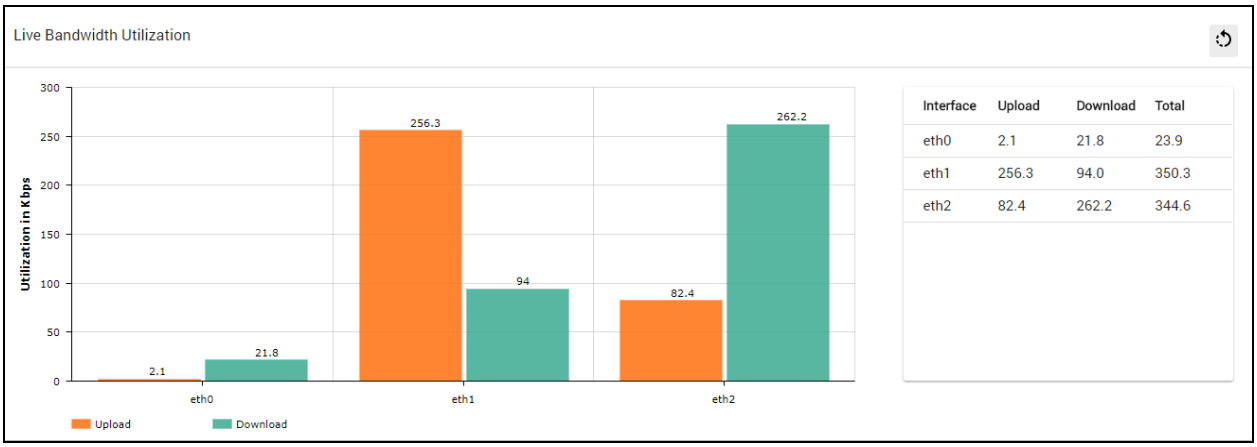
Bandwidth Utilization

You can now view the live bandwidth utilization for each of the network interfaces on the Seqrite UTM in Kbps. Bandwidth utilization statistics can help manage the Internet traffic across the available interfaces. You can also view the historical bandwidth utilization for the available interfaces for hourly, 7 days, and 30 days basis.

1. Navigate to **Logs and Reports > Internet Traffic > Bandwidth Utilization**. In the Live Bandwidth Utilization section, you see the network bandwidth being utilized across the various available interfaces. The upload utilization is displayed in orange color and the download utilization is displayed in green color. The statistics are refreshed every three seconds.



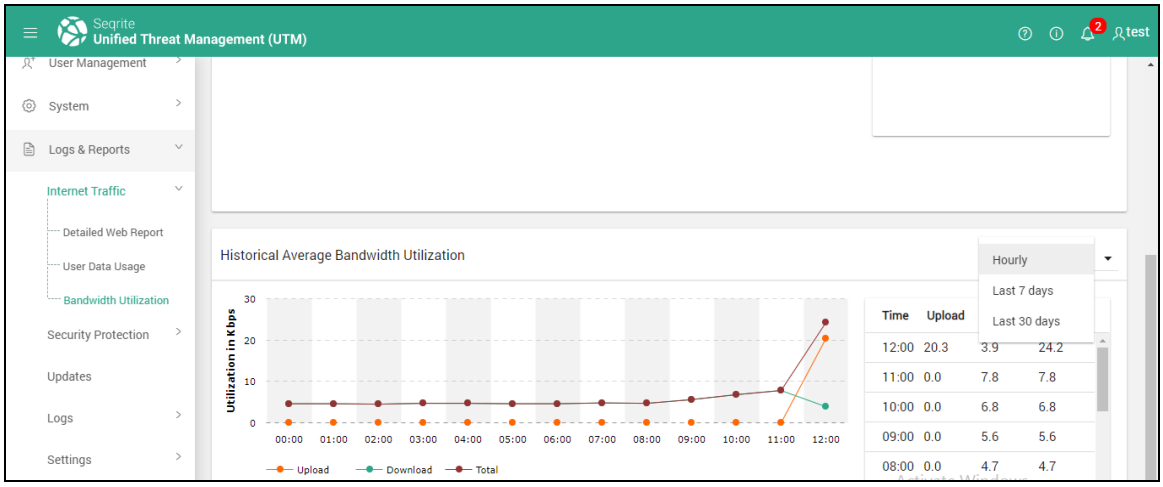
2. To view the Statistics in vertical format, click the **Rotate** icon on the upper right corner.



Viewing Historical Bandwidth Utilization

You can view the historical bandwidth utilization on an hourly, 7 days, and 30 days basis in the Historical Bandwidth Utilization section.

1. Navigate to **Logs and Reports > Internet Traffic**.
2. Click **Bandwidth Utilization**. The historical utilization is displayed below the Live Bandwidth utilization graph. By default, the eth0 interface is selected. You can select any interface from the drop-down to view the corresponding utilization over a selected period.



Security Protection

This section provides various types of reports related to the scanning and protection of emails, firewall intrusion attempts IPS and IDS, reports related to application control, policy breach attempts by users and groups and intrusion attempts. In the logs section, you can access logs related to the current, past and archives logs.

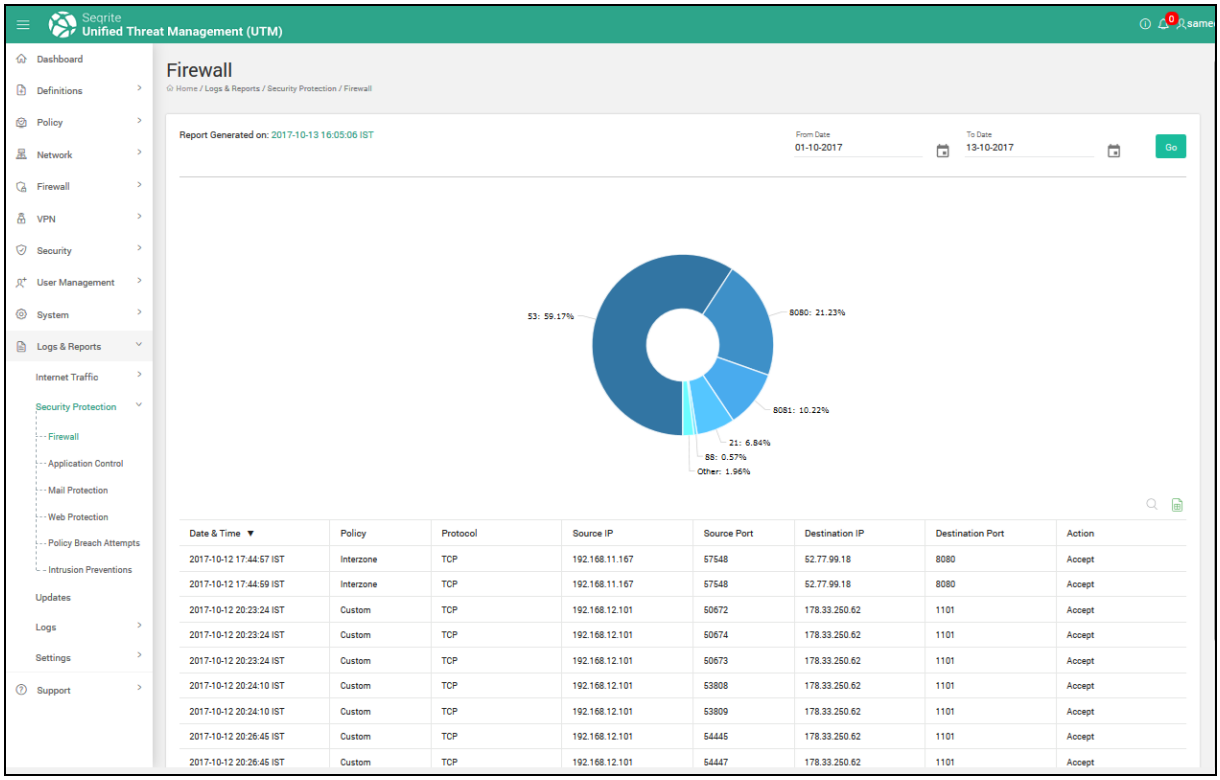
Firewall Reports

The Firewall report displays the information about the internet access / traffic which matches a firewall rule if that rule has the logging option enabled. You can select the time period for viewing the firewall report. The details such as date and time, policy name, Source IP, Source Port, Destination IP, Destination port and the action taken are displayed in the firewall report.

This page also displays a pie chart showing top 5 services (destination ports) accessed through Seqrite UTM. You can also download the report in XLS, Word and PDF format.

Viewing Firewall reports

1. Navigate to **Logs and Reports >Security Protection > Firewall.**
2. Enter/Select the **From Dat**e and the **To Date**.
3. Click **Go.** The Firewall Report for the selected duration is displayed.

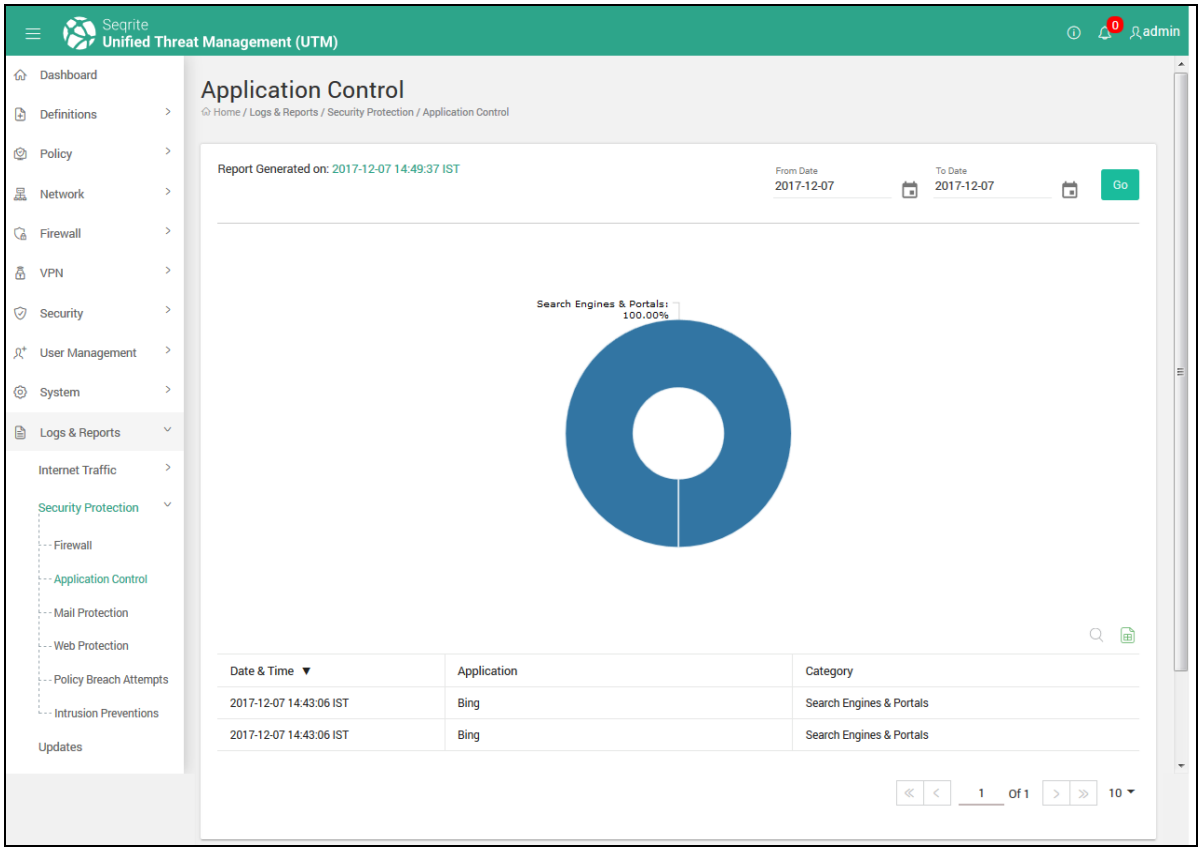


Viewing Application Control Report

The application control report provides information about the applications that are prevented by the Seqrite UTM. It details timestamp of prevented application, application name and associated category.

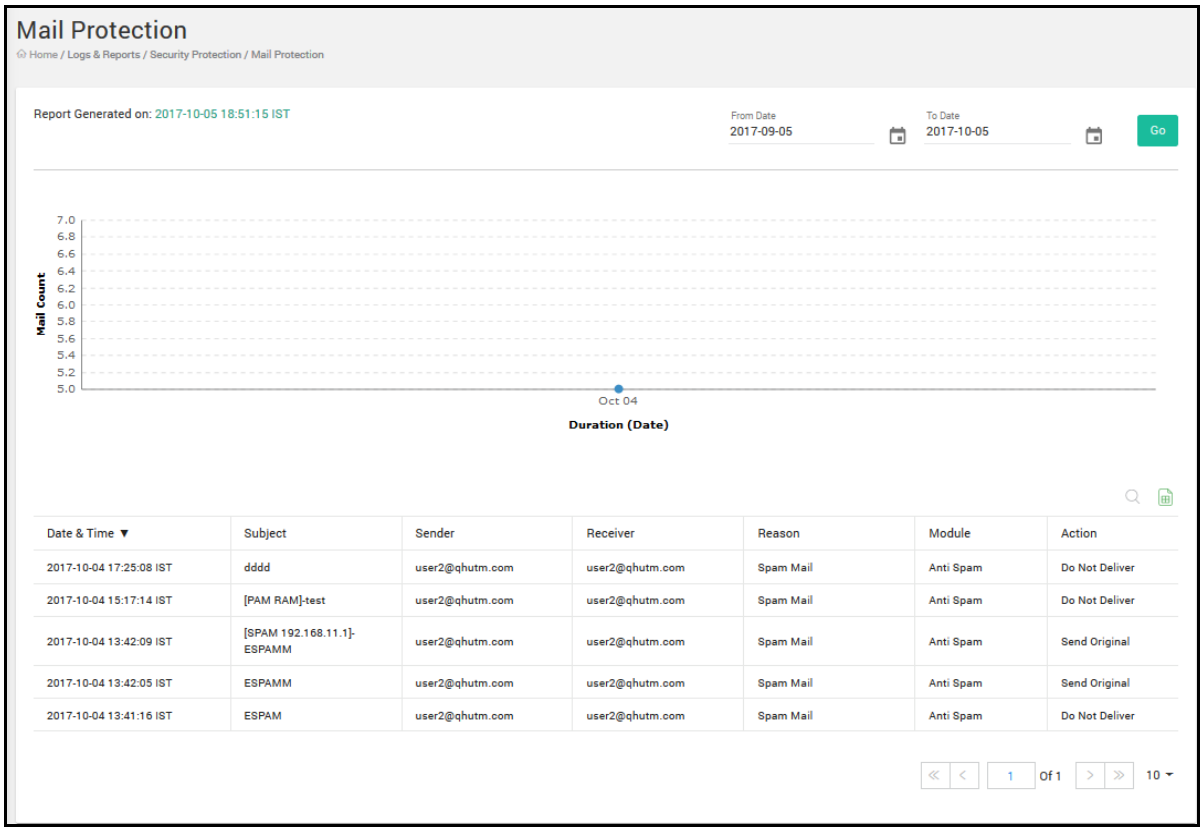
1. Navigate to **Logs and Reports> Application Control.**
2. Enter/Select the **From Dat**e and the **To Date**.

3. Click **Go.** The Application Control Report for the selected duration is displayed.



Viewing Mail Protection Report

Seqrite UTM scans your incoming and outgoing mail for any infections in the attachments. The mail protection report displays the statistics about the scan process for incoming and outgoing mail and includes details about the date and time when the infected mail was sent/received, the sender, the recipient, the subject line, attachments if any and the action taken. You can export this report in excel, PDF and word format.

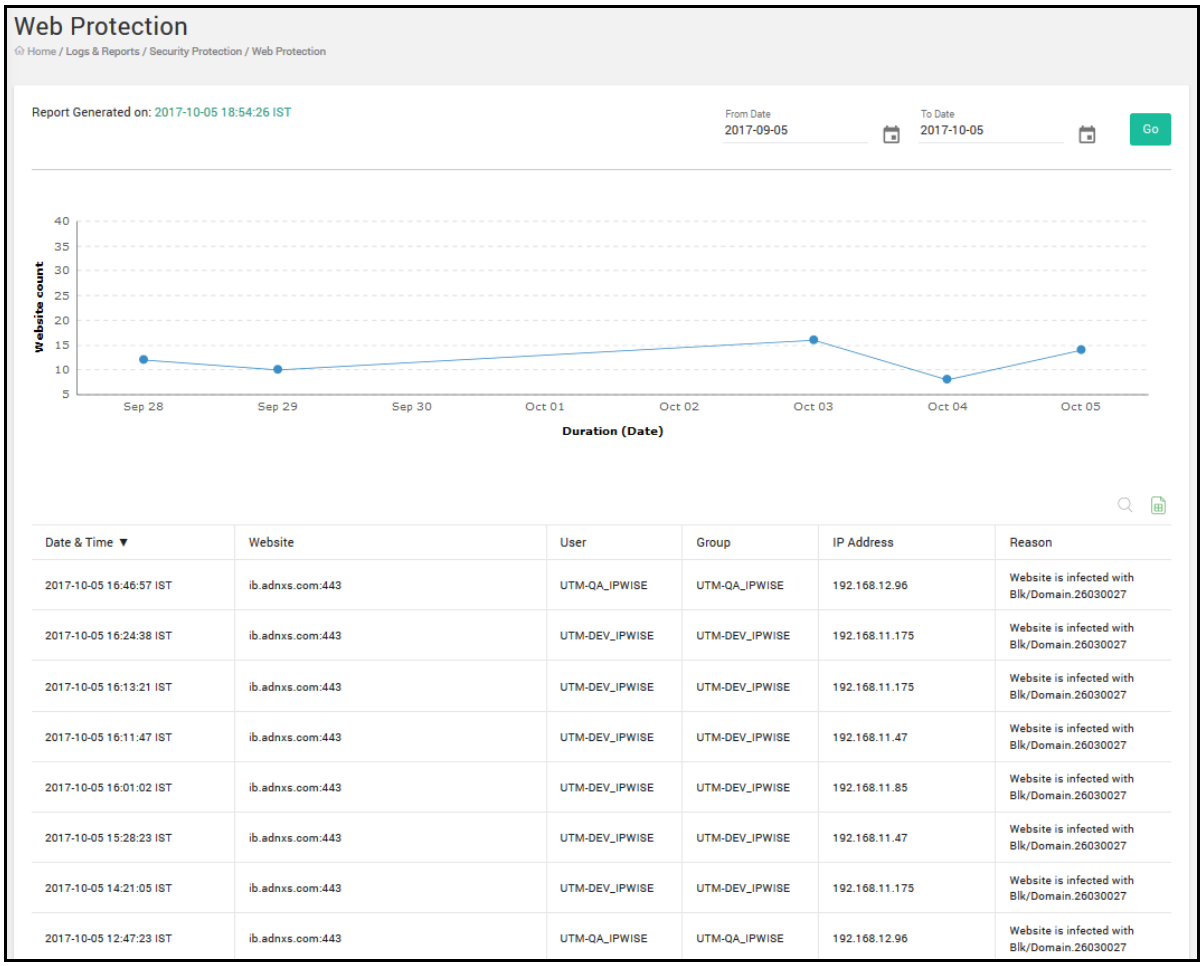


1. Navigate to **Logs and Reports > Security Protection > Mail Protection.**
2. Enter/Select the **From Dat**e and the **To Date**.
3. Click **Go.** The Mail Protection Report for the selected duration is displayed.

Viewing Web Protection Report

The Web protection report gives information about the blocked Web sites, date and time the blocked Web sites were accessed, URLs of the Web sites accessed, and the IP address of the users. It allows to analyze the reason why these sites were blocked. It also details the phishing sites, fraudulent and harmful Web sites accessed by the user.

1. Navigate to **Logs and Reports > Security Protection > Web Protection.**
2. Enter/Select the **From Date** and the **To Date**.
3. Click **Go.** The Web Protection Report for the selected duration is displayed.

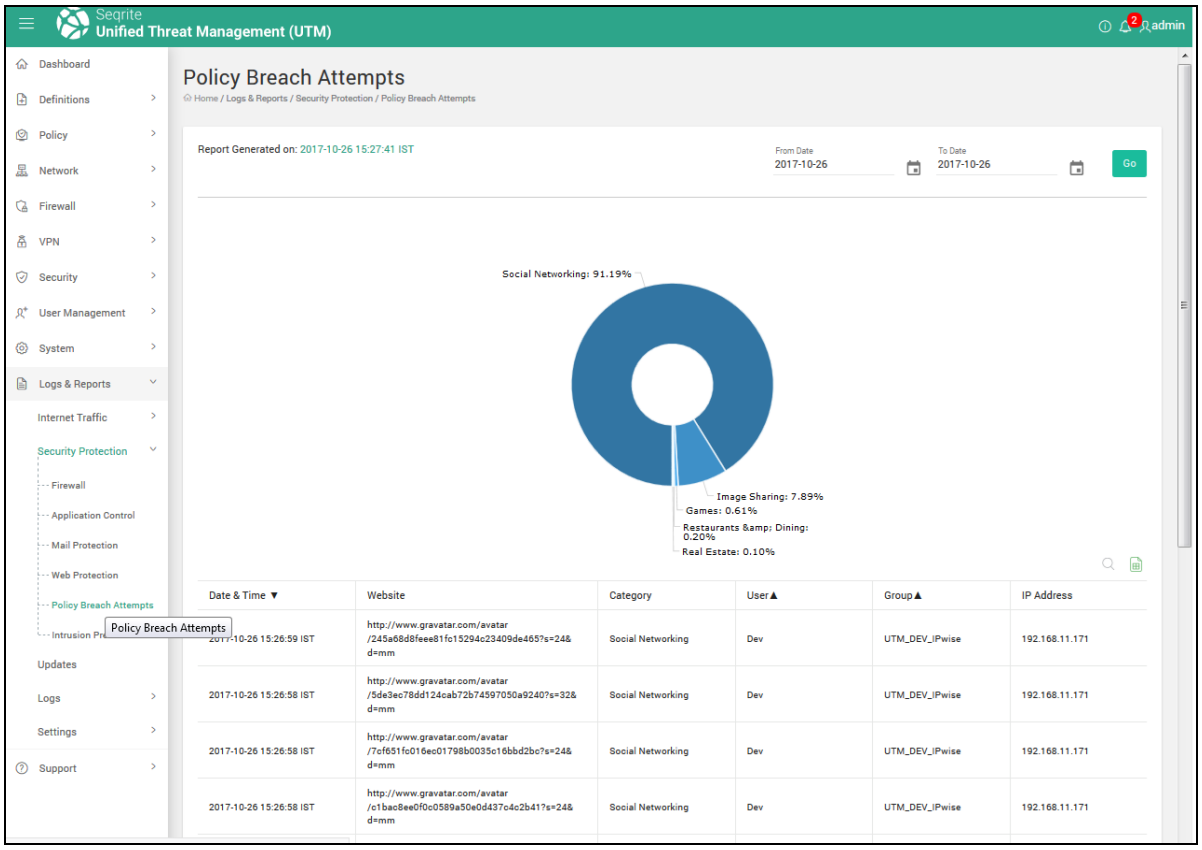


Date & Time ▼	Website	User	Group	IP Address	Reason
2017-10-05 16:46:57 IST	ib.adnxs.com:443	UTM-QA_IPWISE	UTM-QA_IPWISE	192.168.12.96	Website is infected with Blk/Domain.26030027
2017-10-05 16:24:38 IST	ib.adnxs.com:443	UTM-DEV_IPWISE	UTM-DEV_IPWISE	192.168.11.175	Website is infected with Blk/Domain.26030027
2017-10-05 16:13:21 IST	ib.adnxs.com:443	UTM-DEV_IPWISE	UTM-DEV_IPWISE	192.168.11.175	Website is infected with Blk/Domain.26030027
2017-10-05 16:11:47 IST	ib.adnxs.com:443	UTM-DEV_IPWISE	UTM-DEV_IPWISE	192.168.11.47	Website is infected with Blk/Domain.26030027
2017-10-05 16:01:02 IST	ib.adnxs.com:443	UTM-DEV_IPWISE	UTM-DEV_IPWISE	192.168.11.85	Website is infected with Blk/Domain.26030027
2017-10-05 15:28:23 IST	ib.adnxs.com:443	UTM-DEV_IPWISE	UTM-DEV_IPWISE	192.168.11.47	Website is infected with Blk/Domain.26030027
2017-10-05 14:21:05 IST	ib.adnxs.com:443	UTM-DEV_IPWISE	UTM-DEV_IPWISE	192.168.11.175	Website is infected with Blk/Domain.26030027
2017-10-05 12:47:23 IST	ib.adnxs.com:443	UTM-QA_IPWISE	UTM-QA_IPWISE	192.168.12.96	Website is infected with Blk/Domain.26030027

Viewing Policy Breach Attempts Report

The Policy Breach report displays information about any attempts to access Internet against the policies set and implemented by the company. This report is available for a particular day or for last 7 days or for last 30 days. The report provides the date and time of breach, URL of the Web site, and category of the site. With help of this report, the user name, group name, and IP address of the users breaching the policies can be mapped together. You can export this report in excel, word and PDF format.

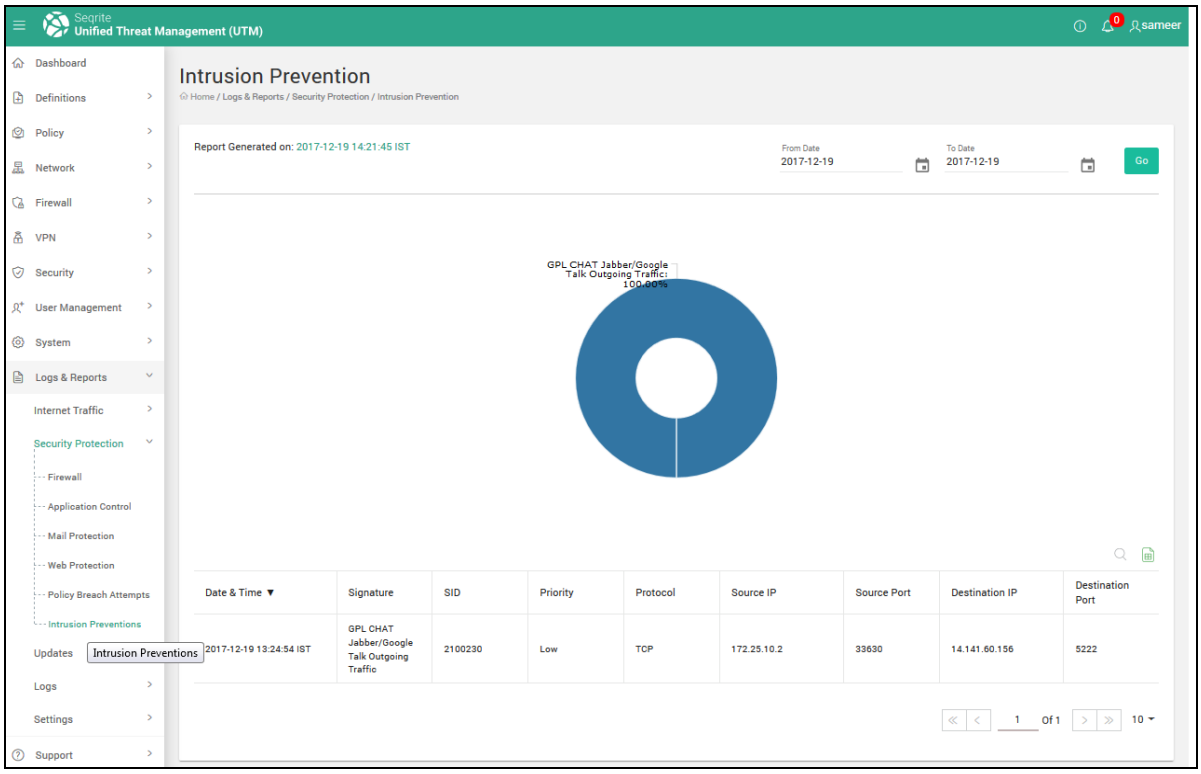
1. Navigate to **Logs and Reports > Policy Breach Attempts.**
2. Enter/Select the **From Date** and the **To Date**.
3. Click **Go.** The Policy Breach Attempts Report for the selected duration is displayed.



Intrusion Prevention Report

The Intrusion Prevention report provides information about intrusions that were prevented by the Seqrite UTM. It details period of intrusion prevention, signature name, activity, priority of the activity, protocol information, and other details. It also identifies problems with security policies, documenting existing threats, and determine individual users from violating security policies.

1. Navigate to **Logs and Reports > Intrusion Prevention.**
2. Enter/Select the **From Dat**e and the **To Date**.
3. Click **Go.** The Intrusion Prevention Report for the selected duration is displayed.

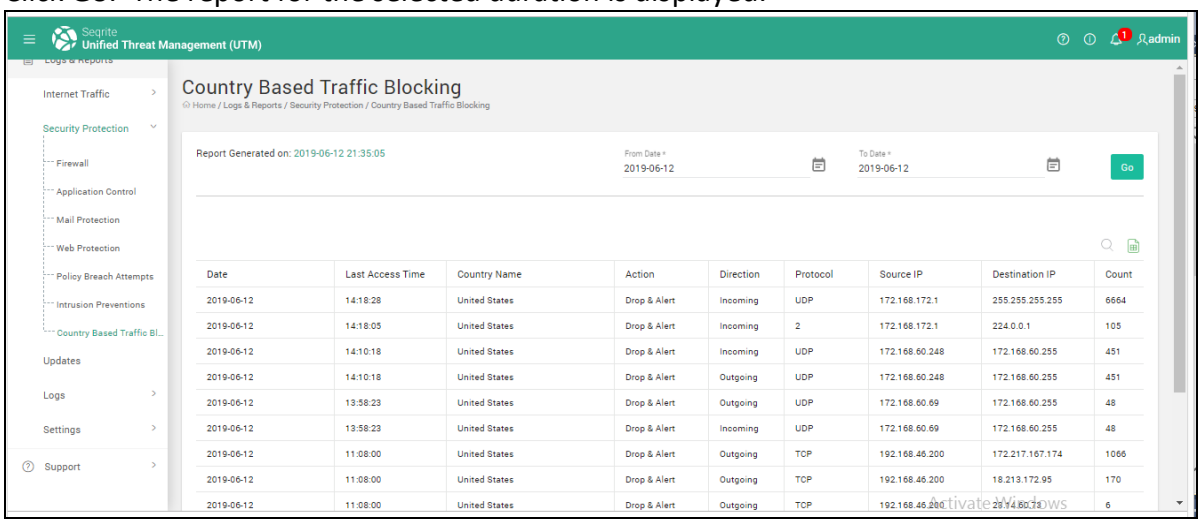


Viewing Country-based blocking breach reports

The Country Based Traffic Blocking report provides information about the breaches made to the country-based blocking rule. It details the Date, Last access times, country name, action configured whether alert or alert and drop, direction whether incoming or outgoing traffic, the protocol, the source and destinations IP addresses, and the count until the last refresh cycle.

1. Navigate to **Logs and Reports > Security Protection > Country Based Traffic Blocking**.
2. Enter/Select the From Date and the To Date.

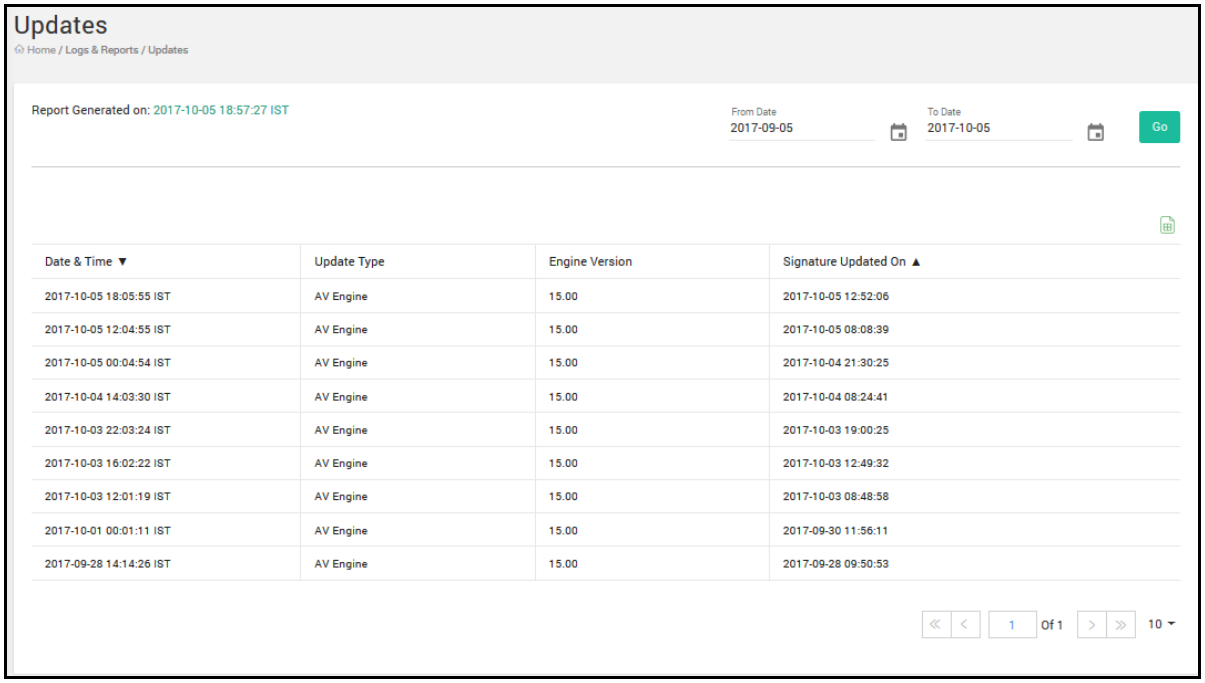
3. Click **Go**. The report for the selected duration is displayed.



Viewing Updates (Database) Reports

This report displays the information about the date and time of the Antivirus and IPS signature updates. After every successful update, a report is generated for update type, Engine version of Antivirus if there is any version update, and the period. Using this report, you can check if the latest Antivirus and IPS signature update is carried on your system. You can export the reports in excel, PDF and word format using the icons provided.

1. Log on to Seqrite UTM. Navigate to **Logs and Reports > Updates.**
2. Enter/Select the **From Dat**e and the **To Date**.
3. Click **Go.** The Updates Report for the selected duration is displayed.



Logs

Use the log viewer on the Seqrite UTM to download and read the log files of the system. You can also select and clear the logs if they are not required. The Log viewer displays all system logs grouped by services and events.

Logs are displayed in three tabbed groups, Live logs, Todays Logs (current logs) and Archived Logs.

- **Live Logs**: Select the module for which you want to view the Live logs from the drop-down. Enable the Autoscroll button if you want the logs to scroll down automatically.

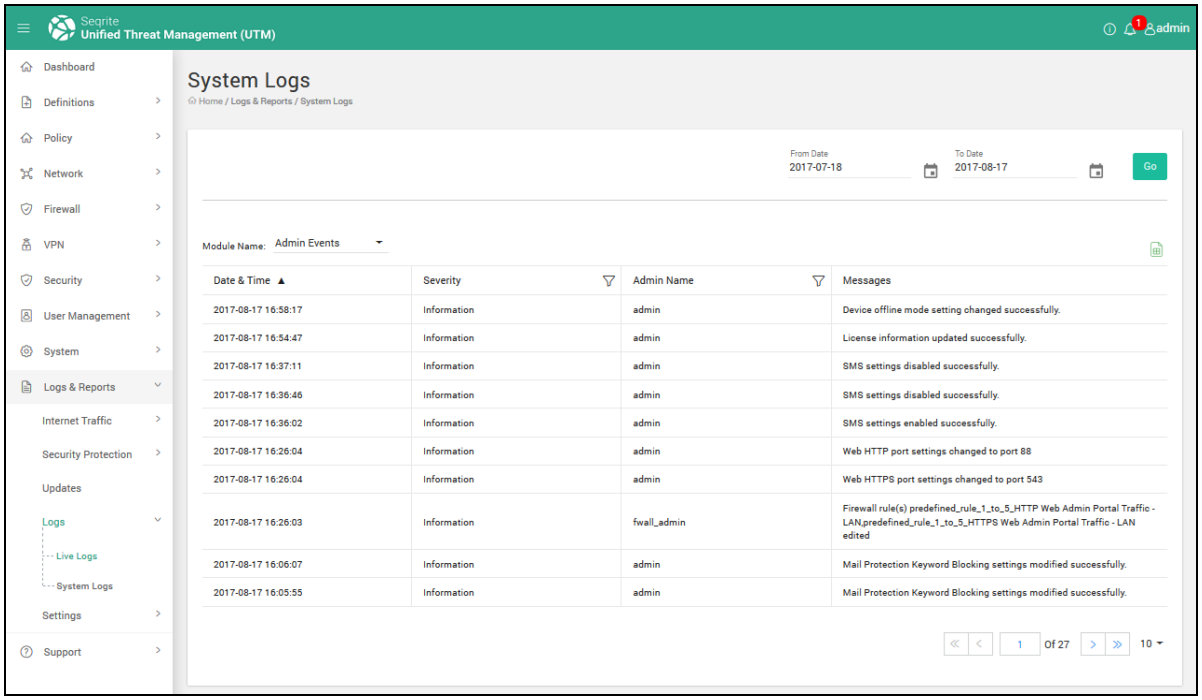
- **System logs tab :** Displays system logs for the current day. These logs include messages generated by Seqrite UTM, user activities, admin activities, updates, logs related to VPN, DHCP and interfaces. You can export the logs if required.

Viewing Live logs

1. Navigate to **Logs and Reports > Live Logs**. The Todays Log page is displayed that contains various logs of Seqrite UTM subsystems along with the module name, log size and log count.
2. To view the current day's logs for a module, click the module name, the relevant logs are displayed with the following details:
   a. The name of the module is shown in the header along with Size and Log Count.
   b. The first column of the page indicates the severity of each log generated, here you can filter the logs according to the severity All, Information, Warning, Error and Critical.
   c. The second column indicates date and time of generation of that log, which can also be sorted.
   d. The third column shows the name of the Admin and the last column displays the actual log message.

Viewing System Logs

1. Navigate to **Logs and Reports > System Logs.** The System Logs page is displayed:



2. Select the **Module Name** from the Module Name drop-down for which you want to view the system logs. The system logs are displayed as per the duration for selected dates.

Log Settings (Purge)

Used for purging (Deleting) old log files

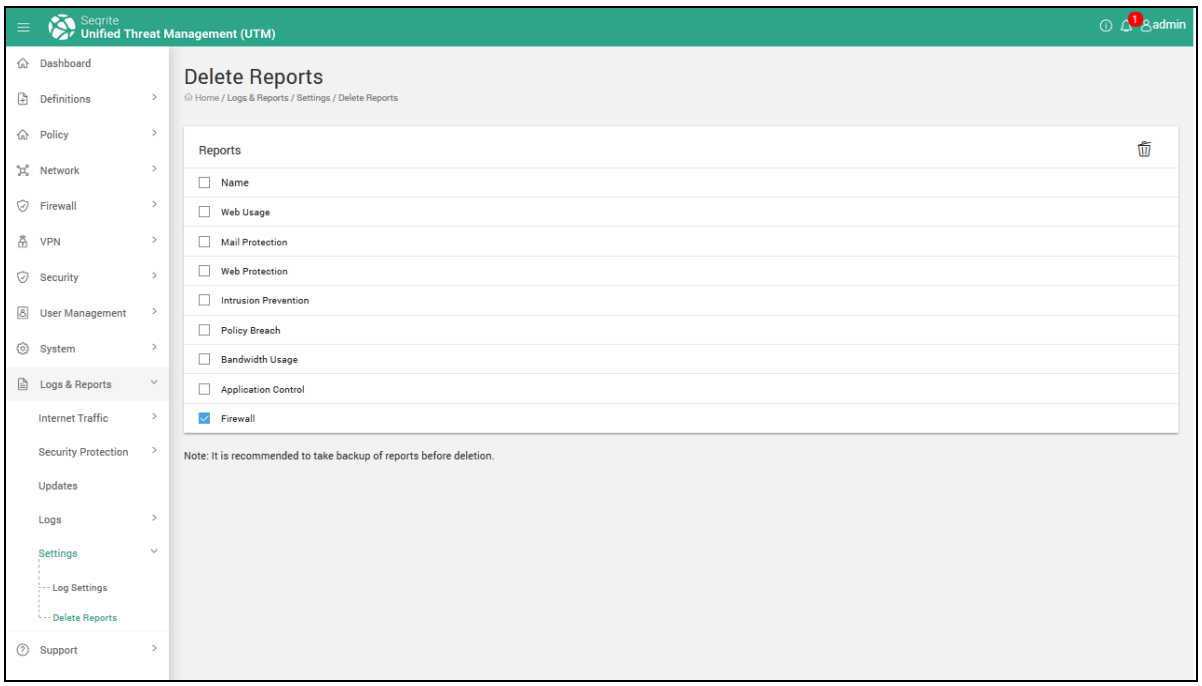
The Settings tab lets you configure the purge cycle to automatically delete the older logs. You can configure the settings to automatically delete the logs that are a day old, logs that are 7 days old, logs that are more than 15 days older, or delete logs that are more than 30 days older.

1. Navigate to **Logs and Reports > Settings > Log Settings.**
2. In the Automatic Log file deletion drop-down, select the required option for e.g Delete logs after 7 days.
3. Click **Save**. Seqrite UTM will automatically delete log files when they have reached the specified age.

Deleting Reports

The **Delete Report** section allows you to delete reports for multiple modules for a specified duration.

1. Navigate to **Logs and Reports > Settings > Delete Reports**.



2. Select the module(s) for which you want to delete reports.
3. Click the **Delete** icon.

4. In the Delete confirmation box, select the duration from one of the following:
   ALL - To delete all reports,
   All except today- to delete all reports except those for today
   Till- To selectively delete reports up to a particular date.

5. Click **Delete**. The reports for the selected criteria will be deleted.

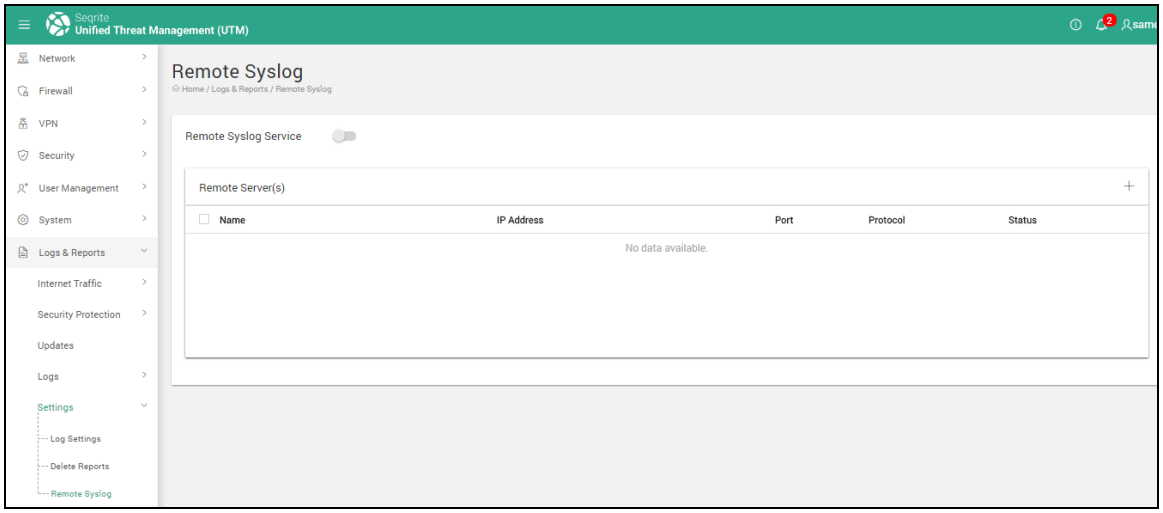
   Note: It is recommended to take backup of the reports before deletion.

Remote Syslog server

You can configure the logs to be sent to the remote syslog server so that the disk space on the UTM is conserved. You can also monitor, analyze the logs on the syslog server independently. Before configuring the remote syslog server on the UTM appliance, you must ensure that the remote server is up and running and the UTM appliance is able to connect to the remote server.

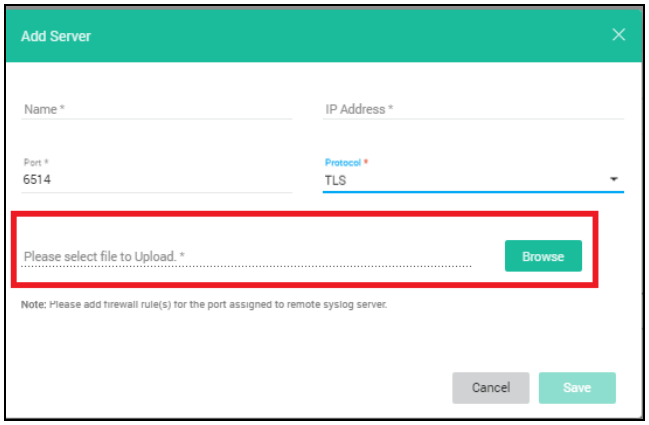
Adding a remote syslog server

1. Navigate to **Logs and Reports > Settings > Remote Syslog Server**.



2. Click the + icon to add a new Syslog server. The Add server dialog box is displayed.
3. Enter the name and IP address of the server.
4. Enter the port number and select the type of protocol using which the log files would be sent to the Syslog server. You can select TCP, UDP or the TLS protocol from the drop-down list.
   Note: To send log files securely, use the TLS protocol. Port number 6514 is automatically configured if you select TLS protocol. Similarly, Port 514 is selected if you select the TCP or UDP protocol.

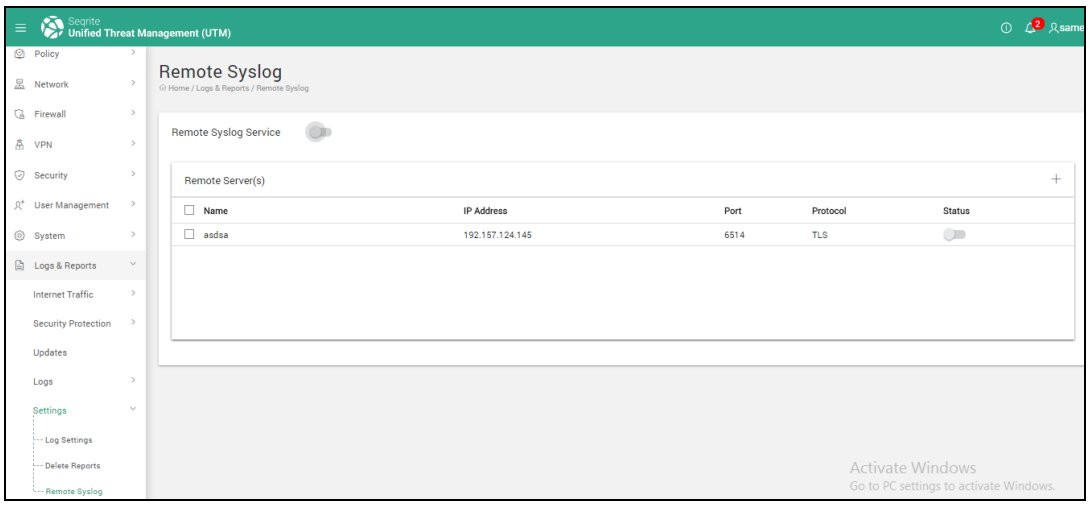
5. Browse and select the certificate file to be uploaded if you have selected the TLS protocol.



6. Click **Save**. The syslog server is added to the list.
   Note: You can add only 2 syslog servers.
   Note: In the Interzone firewall rules, you must the allow the port number which is configured (default is 514) for the syslog communication to happen across the firewall zones if you select TCP and UDP protocols. Similarly, you must allow port 6514 to communicate across the firewall if you select TLS as the protocol.
   See example:
   If the SYSLOG server is running in DMZ zone then the firewall configuration is:
   ALLOW 514 for UDP protocol FROM UTM to DMZ. If the user has selected TCP protocol then configure as ALLOW 514 for TCP protocol FROM UTM to DMZ.

Enabling the syslog service

1. Navigate to **Logs and Reports > Settings > Remote Syslog Server**.



2. Enable the Syslog server from the displayed list of remote servers using the corresponding status toggle button.

3. Enable the Remote Syslog service by toggling the **Remote Syslog Service** status button.
4. Click **Yes** on the confirmation dialog box.
   Note: As soon as you enable the remote syslog server service, the generated system logs will be sent to the configured remote syslog server. Latest Log Reports will be available only on the remote syslog server and will not be available on the UTM appliance.

Chapter

14

Command Line Interface (CLI)

Command line interface (CLI) is a text-based interface that is used to operate software and operating systems. It allows the user to respond to visual prompts by typing single commands into the interface and receiving a reply in the same way.

Configuring Seqrite UTM using the CLI

The Command Line Interface (CLI) console provides a collection of tools to administer, monitor and control certain Seqrite UTM components. There are two ways to access Seqrite UTM using the CLI console:

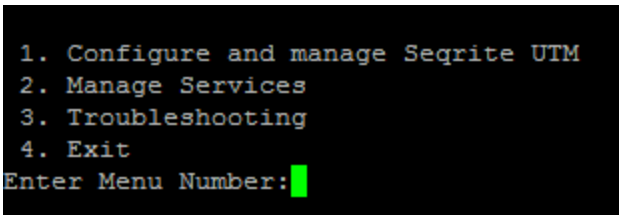
Direct Console connection: This can be done by attaching a keyboard and monitor directly to the Seqrite UTM.

Remote connection: There are two ways of remote connection as follows:

- Accessing CLI console via remote login utility - TELNET
- Accessing CLI console using SSH client

(For more details see Accessing Management interface through Command line interface (CLI).)

On successful login to CLI the Main Menu screen will be shown.



To access any of the menu items, type the number corresponding to the menu item against **Enter Menu Number** and press **Enter**.

Every submenu has a Previous and Exit option. Use **Previous** to go one level up and **Exit** to exit from CLI console.

Command Line Interface (CLI)

The following table explains various menus:

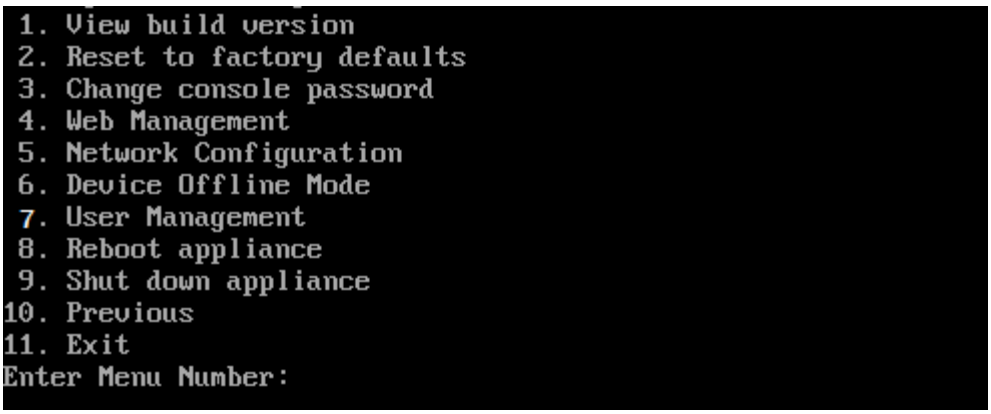
Menu	Description
Configure and manage Seqrite UTM	Helps to configure and manage services available on Seqrite UTM.
Manage Services	Helps to manage services on Seqrite UTM.
Troubleshooting	Helps to troubleshoot services on Seqrite UTM.
Exit	To exit the CLI console.

Configure and manage Seqrite UTM

Seqrite UTM CLI console provides option to configure and manage various services that are available.

To configure and manage Seqrite UTM follow the steps given below:

1. Log in to Command Line Interface **> Configure and Manage Seqrite UTM.**



The following table explains various menus:

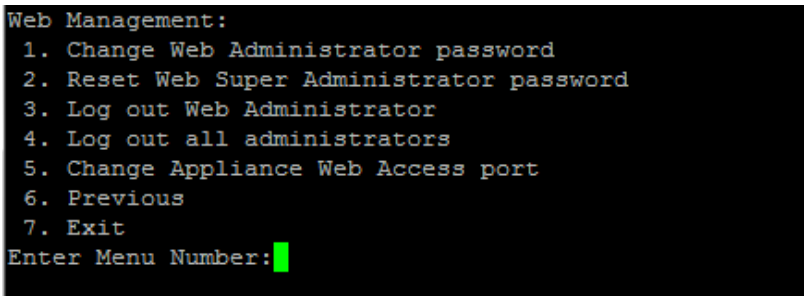
Menu	Description
View Build Version	Use this option to view the Seqrite UTM build version.
Reset to Factory Defaults	Use this option to reset the Seqrite UTM settings to factory defaults.
Change Console Password	Use this option to change the console password.

Web Management	Use this option to explore various options available under Web Management.
Network Configuration	Use this menu to configure your network.
Device Offline mode	Use this option to configure which services will be used offline when no Internet connection is available.
User Management	Use this menu to manage Seqrite UTM users.
Reboot Appliance	Use this option to reboot the Seqrite UTM appliance.
Shutdown Appliance	Use this option to power down the Seqrite UTM appliance.

Web Management

CLI console provides various options for Web Management

1. Log in to Command Line Interface > **Configure and Manage Seqrite UTM > Web Management**.



The following table explains the options available under Web Management:

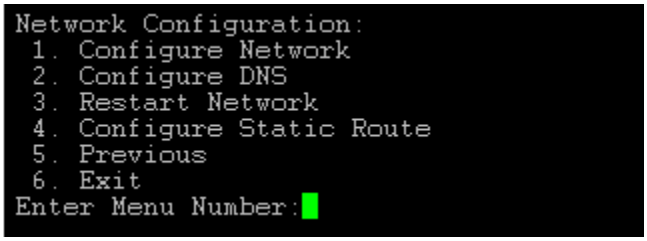
Menu	Description
Change Web Administrator Password	Use this option to change the Seqrite UTM Web Administrator password.
Reset Web Super Administrator Password	Use this option to reset the Seqrite UTM Web Super Administrator password.
Log out Web Administrator	Use this option to logout a Web administrator using the administrator name.

Log out All Administrators	Use this menu to logout all Web administrators.
Change Appliance Web Access Port	Use this option to change the port number(s) for the protocol(s).

Network Configuration

CLI console for Seqrite UTM provides various options for Network. You can use the options to configure network, DNS, Static route and also restart the network.

1. Log in to Command Line Interface **> Configure and Manage Seqrite UTM > Network Configuration.**



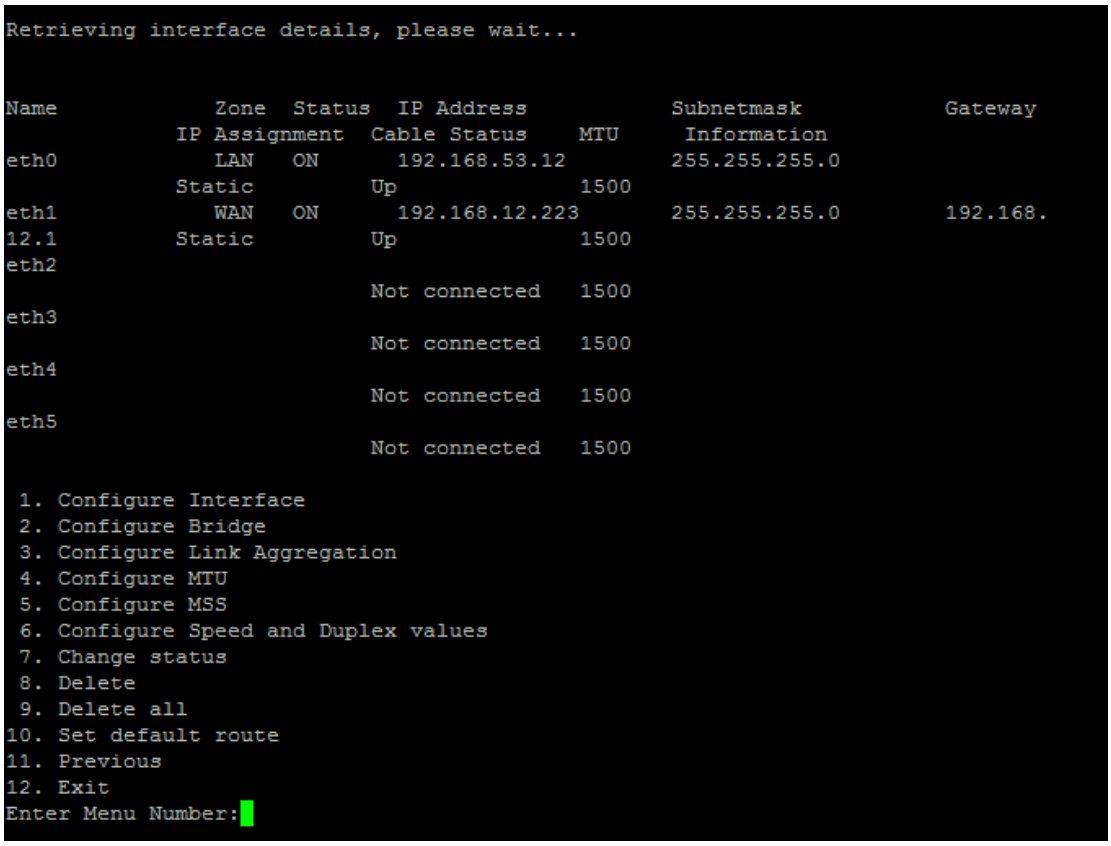
The following table explains the options available under Network Configuration:

Menu	Description
Configure Network	Use this option to configure the Seqrite UTM network. It allows you to configure the LAN and WAN interface settings.
Configure DNS	Use this option to configure the DNS.
Restart Network	Use this option to restart your network.
Configure Static Route	Use this option to configure static route(s).

Configure Network

1. Log in to Command Line Interface **> Configure and Manage Seqrite UTM > Network Configuration > Configure Network.**

Command Line Interface (CLI)



This option retrieves the interface details and provides various options as explained in table below

Menu	Description
Configure Interface	Use this option to configure the Seqrite UTM interface.
Configure Bridge	Use this option to configure a bridge over two interfaces.
Configure Link Aggregation	Use this option top configure Link Aggregation interface.
Configure MTU	Use this option to configure the Maximum Transmission Unit value for your network packet size permitted on your network. Generally, a large MTU value your connections will experience packet loss or dropping Internet connection.
Configure MSS	Use this option to configure the maximum segment size for TCP segments in your network. Generally, packets larger than the MSS value are discarded.
Configure Speed and	Use this option to select the required interface and then set the speed in Mbps, Duplex value whether full or half, Auto

Menu	Description
Duplex value	Negotiation value whether On or Off.
Change Interface Status	Use this option to enable or disable an interface.
Delete Interface / Bridge	Use this option to delete an interface or bridge.
Delete All Interfaces	Use this option to delete all interfaces.
Set Default Route	Use this option to set an interface as default route.

Configure DNS

CLI console provides option to configure DNS. To Configure DNS, follow the steps given below:

1. Log in to Command Line Interface **> Configure and Manage Seqrite UTM > Network Configuration > Configure DNS.**

The following table explains various menus available under Configure DNS:

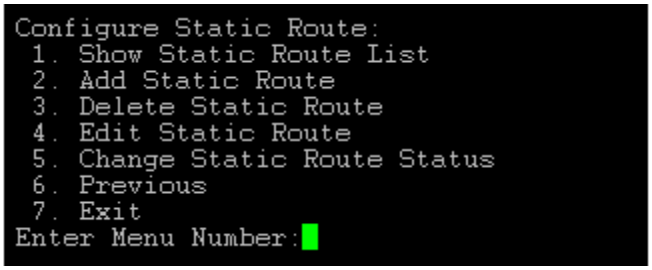
Menu	Description
Show DNS Servers	Displays the information about DNS servers.
Add DNS Server	Use this menu to add a DNS server.
Remove DNS Server	Use this menu to remove a DNS server.

Configure Static Route

CLI console for Seqrite UTM provides various options for configuring static route. To configure static route, follow the steps given below:

1. Log in to Command Line Interface **> Configure and Manage Seqrite UTM > Network Configuration > Configure Static Route.**

Command Line Interface (CLI)

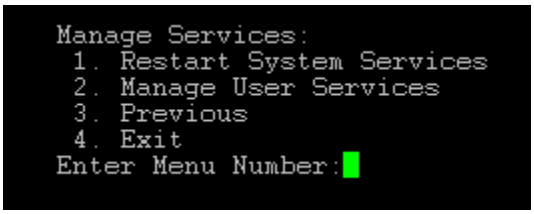


The following table explains the options available under Configure Static Route:

Menu	Description
Show Static Route List	Use this option to see the list of static routes.
Add Static Route	Use this option to add a static route.
Delete Static Route	Use this option to remove a static route.
Edit Static Route	Use this option to edit a static route.
Change Static Route Status	Use this option to change the status of a static route.

Managing Services using the CLI

The CLI console provides options to manage various services of Seqrite UTM as shown in the screenshot below:



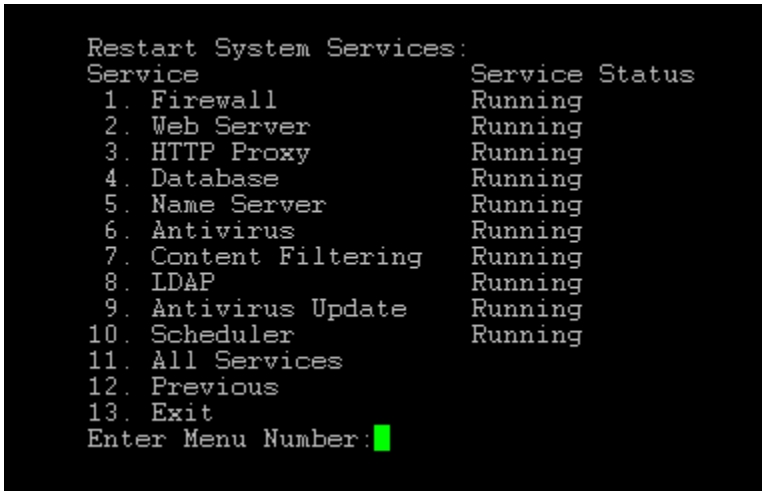
The following table explains various menus available under Manage Services:

Menu	Description
Restart System Services	Use this option to restart system services.
Manage User Services	Use this option to manage user services such as: • IPS • Application control • Policy Based Routing

Restart System Services

Restart System Services allows you to restart any of the system services through CLI.

1. Command Line Interface > **Manage Services > Restart System Services**.

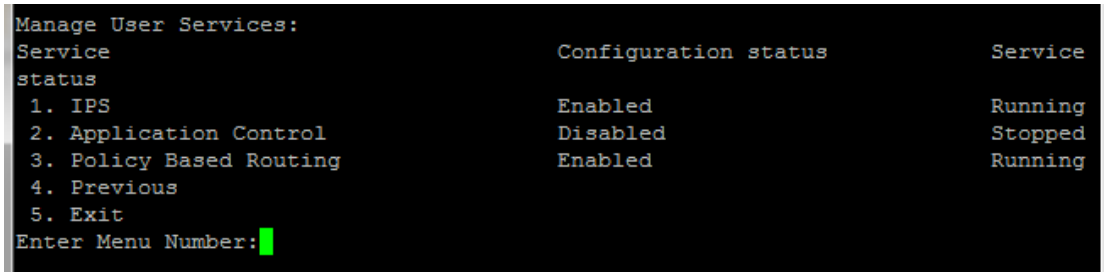


2. Enter the menu number from the list to restart a particular service.

Manage User Services

Using this menu user can manage various user services.

1. Log in to Command Line Interface > **Manage Services > Manage User Services.**

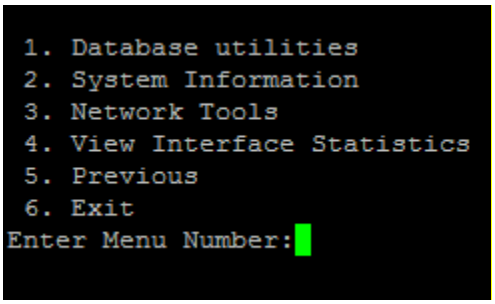


The following table explains various menus available under Manage User Services:

Menu	Description
IPS	Use this option to enable, disable or restart IPS.
Application Control	Use this option to enable, disable or restart Application Control.
Policy Based Routing	Use this option to enable, disable or restart Policy Based Routing.

Troubleshooting using the CLI

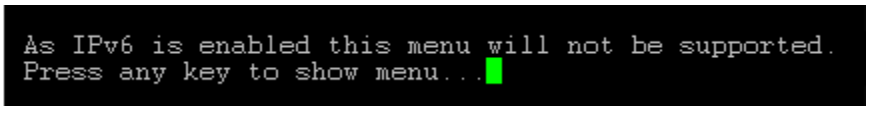
The CLI console on the Seqrite UTM provides options to troubleshoot various services of as shown in following figure.



The following table explains the commands used for troubleshooting:

Menu	Description
Database Utilities	Use this option to explore various database utilities available.
System Information	Use this option to view system information.
Debugging Information	Use this option to collect debugging information of the different modules in Seqrite UTM.
Network Tools	Use this option to view the available network tools.
View Interface statistics	Use this option to view the interface statistics such as Errors, Dropped Packets, Collisions, Duplex, Interface Speed, Rx and Tx Packets/Bytes
Note: If IPv6 is enabled, following modules from CLI console will not be accessible: Configure & Manage Seqrite UTM >> Reset to Factory Defaults Configure & Manage Seqrite UTM >> Network Configuration Troubleshooting	

The following message is displayed if IPV6 is enabled on system.



Troubleshooting Database Utilities

1. Log in to Command Line Interface **> Troubleshooting > Database Utilities**.
2. Seqrite UTM CLI console provides various database utilities as shown in figure below:

Command Line Interface (CLI)

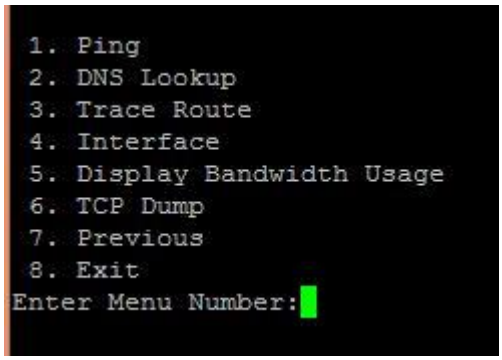
The following table explains various menus available under Database Utilities:

Menu	Description
Web reports	Use this option to repair or clean database for Web reports.
Mail Protection	Use this option to repair or clean database for Mail Protection.
Web Protection	Use this option used to repair or clean database for Web Protection.
IPS Reports	Use this option to repair or clean database for IPS reports.
Policy Breach	User can use this option to repair or clean database for Policy Breach.
Update Reports	Use this option to repair or clean database for Update reports.
Firewall	Use this option to repair or clean database for Firewall reports.
Bandwidth Reports	Use this option to repair or clean database for Bandwidths reports.
Application control reports	Use this option to repair or clean database for application control reports.
Logs	Use this option to repair or clean database for Log reports.
All	Use this option to repair or clean database for All modules.

Troubleshooting Network Tools

To troubleshoot Network tools, follow the steps given below:

1. Log on to Command Line Interface **> Troubleshooting > Network Tools.**



The following table explains the various menus available under Network Tools

Menu	Description
Ping	Use this option to ping a particular IP address.
DNS Lookup	Use this option to lookup a particular IP address.
Traceroute	Use this option to route packets trace to network host.
Interface	Use this option to get all the necessary information about configured interfaces.
Display Bandwidth Usage	Displays the total bandwidth usage for incoming and outgoing traffic for a selected interface.
TCP Dump	Use this tool to capture and analyze packets passing through a particular interface, to or from a particular host, source, destination, port, specific protocol, to save TCP dump contents to a particular file for later use.

Chapter 15

Support

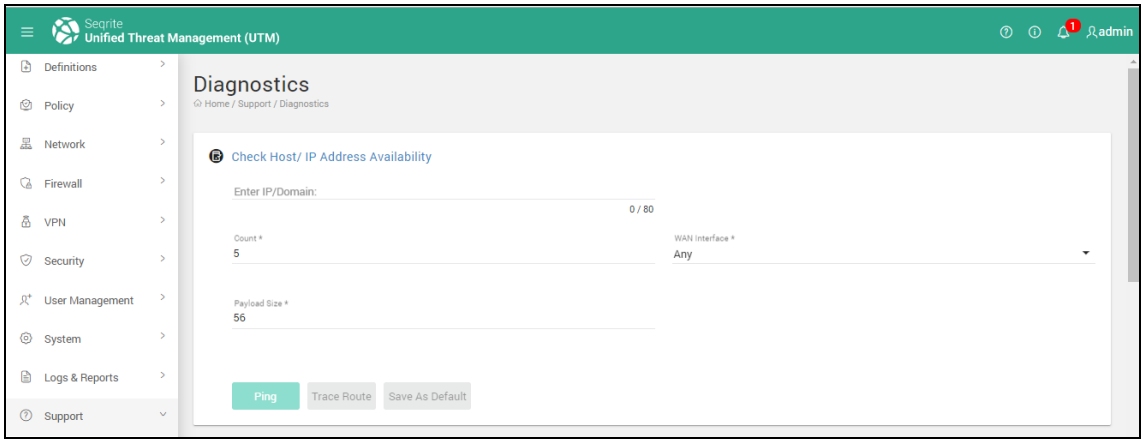
Diagnostics

Before submitting a support ticket, you must check and verify host/ IP Address availability using diagnostic tools. Seqrite UTM lets you perform some diagnostic tests such as check Host/IP address availability.

Checking host availability/IP address

Before submitting a support ticket, you must check and verify host/ IP Address availability using diagnostic tools. The connectivity to any IP address can be checked as follows:

1. Navigate to **Support > Diagnostics.** The Support page is displayed.



2. Enter the **IP/Domain**.
3. Enter the applicable count and select interface if specific.
4. Enter the payload value.
5. Click **Ping** to check the whether the host is reachable.
6. Click **Trace Route** to check the route (path) and transit delays of packets.

Bypass security policies

Sometimes you may require to bypass the Seqrite UTM during troubleshooting purposes. You can click the Status button to activate the bypass option. If you enable this option, all traffic will be bypassed from LAN to WAN without any restrictions and security policies.

Note: You must remember to turn off the Bypass security policies button after you complete your troubleshooting.

1. Navigate to **Support > Diagnostics.**
2. In the Bypass security policies section, toggle the status switch for enable bypassing security policies. Note: You must remember to turn off the Bypass security policies button after you complete your troubleshooting.

Getting /Reporting URL Categorization

This tool lets you find out the category of a particular URL. If you feel that a particular URL is categorized incorrectly, you can choose to report it.

1. Enter the URL in the designated textbox.
2. Click **Get Category**. The category of the URL is displayed.
3. To report an incorrectly categorized website, click the **Report Miscategorization** button.

Port Mirroring

Port mirroring is a method used by Network administrators to analyze and debug data or diagnose errors on a network. It helps in monitoring network traffic by copying packet from one port on a network device to another port where the packets can be analyzed. Port mirroring helps the administrators to keep a close eye on network performance and alerts them when problems occur. It can be used to mirror either inbound or outbound traffic (or both) on interfaces.

You can configure port mirroring on Seqrite UTM by assigning a source port from which you want to copy all packets and a destination port (known as the Mirror port) to which the copied packets will be sent. All the packets received on the source port are forwarded to the destination port. You can attach an analyzer on the destination (mirror) port to monitor each segment separately. The analyzer captures and evaluates the data without affecting the client on the original port.

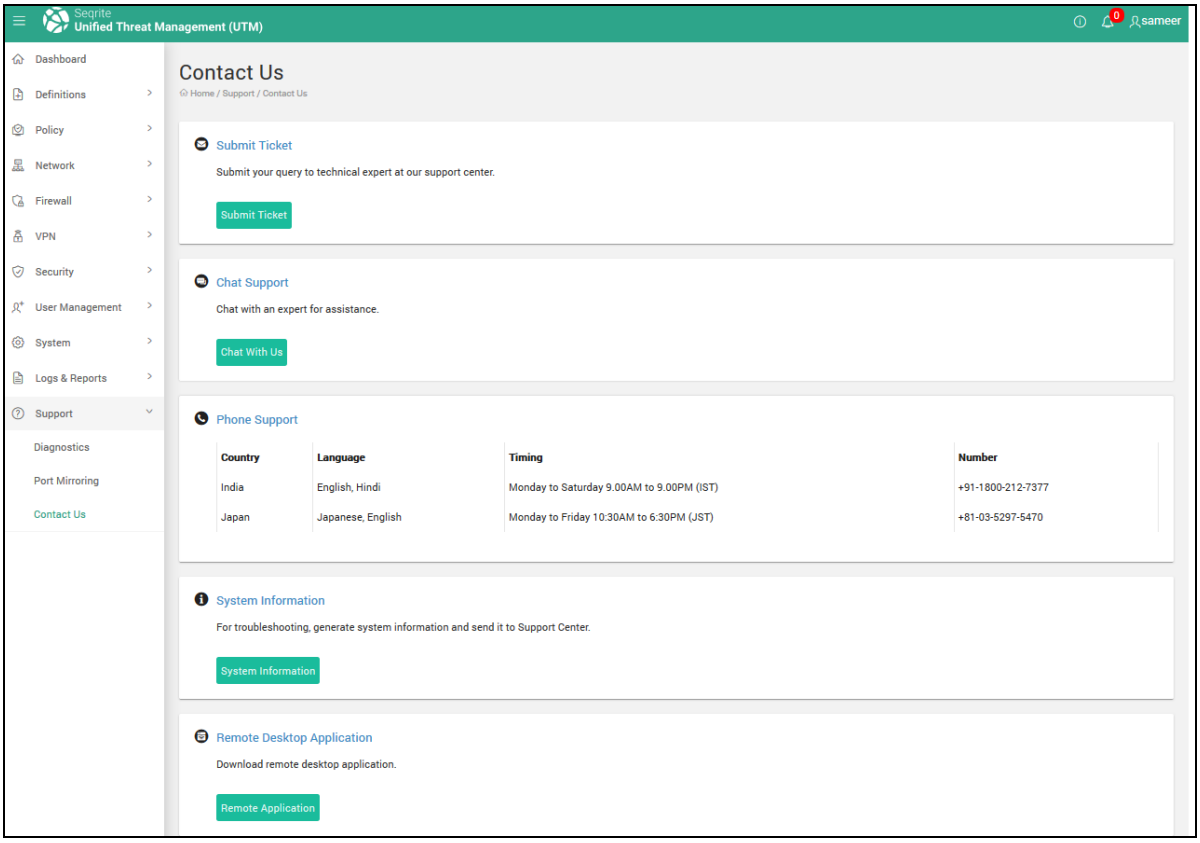
Configuring port mirroring

1. Navigate to **Support > Port Mirroring**. The Support page is displayed.
2. Toggle the Port Mirroring status to enable port mirroring.
3. Click the **+ (Add) icon** to add port mirroring details.

4. Select the source interface.
5. Select the destination interface. This should be a LAN port.
   Note: eth0 cannot be set as destination (mirror) port.
6. Select the Direction of network traffic. Here you can select traffic as inbound, outbound or both.
7. Select the **Protocol** and click **Add**. You can filter traffic based on the protocols on which the traffic is being sent.
8. Click **Save**.

Support - Contact Us

Using the Support page, you can report a problem or issue related to the Seqrite UTM. The following support options are available:



Submit Ticket

Click Submit Ticket to submit information about your issue to Seqrite Support. You will be redirected to the Seqrite Support & Services site. Search the knowledge base in the knowledge database login or signup to submit your issue to Seqrite Support.

Chat Support

Using this option, you can chat with our experts who are there online to assist you. You will be redirected to the Seqrite Support site where a host of options are available to you. Use the Chat with us option to chat with our support team member regarding your issue.

Phone support

Using this support type, you can call the technical support center for instant support. The numbers, language available, and the support timings for the countries are as follows.

Seqrite users (India): +91 1800 212 7377 Monday to Saturday 9.00 Am to 9.00 PM (IST) Languages: English and Hindi

Support

Seqrite users (Japan): 81-03-5297-5470 Monday to Friday 10.30 AM to 06.30 PM (JST)

Languages: English and Japanese

System Information

Alternatively, you can also download a log file containing vital information related to your appliance and send it to the Seqrite Support team, so that they can analyse your issue and find a solution. Click System Information to generate a report.

Remote Desktop application

You can also choose to download our Remote access application and install it on your appliance. This application will install the Team Viewer support application on your appliance. This application will help Seqrite Support take remote control of your desktop and troubleshoot your system. After you install the application, a unique ID and password will be generated for your computer. You have to share the ID and the password with the Seqrite Support staff, who will then use the credentials to connect to your appliance remotely for troubleshooting.

Details required during the call:

- Product Key: If purchased online, it can be obtained from the email confirming the order.
- Information about your computer system: brand, processor type, RAM capacity, the size of the hard drive and free space on it, as well as information about other peripherals.
- The operating system: name, version number, language.
- Version of the installed anti-virus and the virus database.
- Software installed on your system.
- Is your system connected to a network? If yes, contact the system administrators first. If the administrators cannot solve the problem, they should contact the Seqrite technical support.
- Details: When did the problem first appear?

Help Ver. 2.3.0.1

Head Office Contact Details

Quick Heal Technologies Limited

(Formerly known as Quick Heal Technologies Pvt. Ltd.)

Reg. Office: Office No. 7010 C & D, 7th Floor, Marvel Edge, Viman Nagar, Pune 411014.

Email: info@seqrite.com

For more details visit: www.seqrite.com

Index

Index

Document last updated on January 15, 2020