Seqrite

TERMINATOR v1.8

Admin Guide

www.seqrite.com

Copyright Information

This document is current as of the initial date of publication and may be changed by Quick Heal at any point of time.

Trademarks

End-User License Agreement

Seqrite Terminator (Unified Threat Management or UTM) End-User License Agreement

IMPORTANT

PLEASE READ THIS SEQRITE TERMINATOR (UNIFIED THREAT MANAGEMENT OR UTM) END-USER LICENSE AGREEMENT (HEREINAFTER REFERRED TO AS THE “AGREEMENT”) CAREFULLY BEFORE USING OR TRYING TO ATTEMPT TO USE THIS SEQRITE TERMINATOR (HEREINAFTER REFERRED TO AS “TERMINATOR”). THE END USER LICENSE AGREEMENT IS MADE AVAILABLE TO YOU AT THE TIME OF PRODUCT ACTIVATION AND IS ALSO AVAILABLE AT www.seqrite.com/eula.

BY USING TERMINATOR OR BY SELECTING THE "I AGREE" OPTION OR ATTEMPTING TO/CONSENTING TO INSTALL TERMINATOR IN ANY WAY, (SUCH ACTION WILLL CONSTITUTE A SYMBOL OF YOUR CONSENT AND SIGNATURE), YOU ACKNOWLEDGE AND ADMIT THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. THIS AGREEMENT ONCE ACCEPTED BY “YOU” [AS AN INDIVIDUAL (ASSUMING YOU ARE ABOVE 18 YEARS AND/OR HAVING LEGAL CAPACITY TO ENTER INTO AN AGREEMENT), OR THE COMPANY OR ANY LEGAL ENTITY THAT WILL BE USING TERMINATOR (HEREINAFTER REFERRED TO AS 'YOU' OR 'YOUR' FOR THE SAKE OF BREVITY)] SHALL BE A LEGALLY ENFORCEABLE AGREEMENT BETWEEN YOU AND QUICK HEAL TECHNOLOGIES LIMITED (FORMERLY KNOWN AS QUICK HEAL TECHNOLOGIES PVT. LTD.) PUNE, INDIA (HEREINAFTER REFERRED TO AS “QUICK HEAL”) AND YOU SHALL HAVE THE RIGHTS TO USE TERMINATOR SUBJECT TO THE TERMS AND CONDITIONS MENTIONED IN THIS AGREEMENT OR AS AMENDED BY QUICK HEAL FROM TIME TO TIME. IF YOU DO NOT AGREE TO ALL THE TERMS AND CONDITIONS BELOW, DO NOT USE TERMINATOR IN ANY WAY AND PROMPTLY RETURN THE SAME (WITHOUT USING THE SAME) IN YOUR POSSESSION.

Seqrite Terminator is a software product developed by Quick Heal. In consideration of payment of the license fee, evidenced by the receipt, Quick Heal grants You, a non-exclusive and non-transferable right to use of Terminator during the license period (as stated in your invoice) a Unified Threat Management solution, according to the technical requirements described in the user manual and which is subject to the terms and conditions of this Agreement.

1. TERM

You are entitled to use Terminator only during the license period commencing from the date of activation of Terminator upto the period mentioned in your invoice details. Except for evaluation and beta licenses or other licenses where the term of the license is limited per the evaluation/beta or other agreement, the term of the license is for the duration mentioned in your invoice.

2. EVALUATION AND REGISTRATION

You are hereby licensed to use this non-transferable, non-exclusive, non-sub-licensable software / Terminator. Use of this software / Terminator beyond the said period is in violation of Indian and international copyright laws.

Quick Heal reserves all rights not expressly granted, and retains all intellectual property and proprietary rights, title and ownership of the software / Terminator, including all subsequent copies in any media. This software / Terminator and the accompanying written materials are the property of Quick Heal and are copyrighted. Copying of the Software or the written material is expressly forbidden.

3. RESTRICTIONS

You are liable for risk of loss or damage of Terminator while it is in your possession or control. You (including your employees, agents, contractors not authorized by Seqrite) agree not to:

a. emulate or adapt any portion of Terminator/software.

b. debug, decompile, modify, translate and reverse engineer Terminator/software.

c. try making an attempt to reveal/discover the source code of the software.

d. create derivative works based on Terminator/software or any portion thereof with sole exception of a non-waivable right granted to You by any applicable legislation.

e. remove or alter any copyright notices or proprietary notices on any labels, or marks of Terminator, software.

f. reduce any part of the software to human readable form.

g. demonstrate, copy, or sell Terminator/software to any third party.

h. publish or otherwise disclose information relating to the performance or quality of the Terminator/software to any third party.

i. sublicense, rent or lease any/all portion of Terminator/software.

j. use for an unlicensed and illegal purpose.

k. assign or transfer any of your rights or obligations under this Agreement.

4. ACTIVATION / INSTALLATION

a. Seqrite will install Terminator onsite or through remote support. You must follow the steps mentioned in Quick Start Guide for Terminator. Seqrite expressly disclaims any loss of data, loss of profits during such installation. If you modify your device or make alterations/modifications to other vendors' software installed on it, you may be required to repeat the activation of the software or the installation of the license key file or in case contact Seqrite Support. Seqrite reserves the right to verify the validity/legality of license and software.

b. Seqrite will verify the device submitted by the user at the time of registration, if there are problems related to verification, the product will not be activated / installed. The verification process is essential for activation of the product.

5. THIRD PARTY WEBSITE LINKS / APPLICATIONS

The software/ terminator product may include links to third-party websites and open source free applications; you may be redirected to such third-party websites / open source applications as a user of this software / terminator. The third party sites / applications are not under the control of Seqrite and Seqrite is not responsible for the contents / any links of any third party-website and use of applications. Seqrite is providing these links to the third-party websites / use of applications to you only for your convenience and is not responsible for any kind of loss/ damage arising out of it.

6. OPEN SOURCE SOFTWARE LICENSES

This Software / Terminator may include some software programs that are licensed (or sublicensed) to the user under the GNU GENERAL PUBLIC LICENSE VERSION 2 (GPL v2), Apache license V2, OPENVPN License, BSD 2.0, IBM Public License 1.0, ISC, GNU Lesser General Public License 2.1 (LGPL 2.1), MIT, The OpenLDAP Public License, OpenSSL Combined License, The PHP License, version 3.01, ZLIB/LIBPNG LICENSE or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). Seqrite reserves the right to use or opt for any version of any Open Source Software either for providing update or otherwise. If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to tpsrc@quickheal.com or the source code is supplied with the Software. The information and licenses of the open source software can be accessed from the link www.seqrite.com/eula. If any Open Source Software licenses require that the Right holder provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

The lists of the open source applications used in the Software along with respective licenses are provided at the end of Agreement. Seqrite may update this list from time to time.

7. SUPPORT

Seqrite offers support features during usage of this software / Terminator i.e., Live Chat with technical support team and/ or the technical support team may, at your discretion, take remote access of your device. The availing of this support will be solely at your discretion and you are solely responsible to take backup of the existing data/software/programs in your device before availing of remote support. Seqrite will not be held responsible for any loss of data, any kind of direct/ indirect/ consequential loss or damage to data/ property arising during this entire process. If at any point of time, the Technical Support team is of the opinion that the issue is beyond their scope, it will be the sole discretion of Seqrite to suspend, cease, terminate, or refuse such support as Seqrite does not provide any warranty and/or guarantee of any kind related to providing support.

8. EMAIL/ELECTRONIC COMMUNICATION

After you register the software / Terminator by activating / installing the software / Terminator, Seqrite may communicate with you on the contact information submitted during the registration process through email or any other electronic communication device. The communication can be for the purpose of product verification for your convenience.

9. SEQRITE STATUS UPDATE

Upon every update of licensed copy, Seqrite Update module will send current product status information to Seqrite Internet Center. The information that will be sent to the Internet Center includes the Seqrite protection health status such as whether the monitoring service is working as expected. The information will be used to provide quick and better technical support for legitimate customers.

All the registered users/subscribers will get the updates free of cost from the date of license activation until the expiry date of the license.

10. COLLECTION OF INFORMATION

Seqrite software / Terminator may collect the following information that may / may not contain any personally identifiable information either with or without your discretion/permission for statistical purpose or enhancing and evaluating the ability, effectiveness and performance of Seqrite's product in identifying and/or detecting the malicious behavioral pattern, inherently fraudulent websites and other Internet security threats/ risks. Password entered by the end users during registration is not stored on the Seqrite server. This information will not be correlated with any personally identifiable information except as herein stated and shall include, but not be limited to:

a. Any type of executable files that the software / Terminator may identify having a potentially malware behavior pattern.

b. Any type of information related to the status of the software / Terminator such as whether there occurred any error while installing the software or the installation was successful.

c. Any type of URLs of the websites that the end users visited that the software deems inherently and potentially fraudulent.

d. Any type of information that software deems potentially fraudulent, posing security risks/ threats.

e. Any type of information for identifying the Media Access Control (MAC) address of the device, Global Positioning System (GPS) on which the software / Terminator has been installed.

f. Any type of information for identifying the Internet Protocol (IP) address and information required for effective license administration and enhancing product functionality and usability.

g. You admit that the information/data as collected above can be used for analyzing, preventing and detecting the potentially internet security risks, publishing any type of data/ reports/ presentations on the trends collected, and sharing the data to create awareness with any organizations and vendors.

11. LIMITED WARRANTY AND DISCLAIMERS

This software / Terminator package is provided as such without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness of the package. In no event will Seqrite or its suppliers will be liable to you or anyone else for any damages arising directly/indirectly or consequential, including loss of data, lost profits or any other damages of data/ property arising out of the use or inability to use this software package ever. Seqrite reserves the right to co-operate with any legal process and may provide documents, information related to your use of this Software. The disclaimers and limitations set forth above will apply regardless of whether you accept the software.

This is an abridged version/extract of Seqrite Terminator End-User License Agreement. It is recommended that you read the terms of our software usage license agreement in details before actually using the software. For detailed version of Seqrite Terminator End-User License Agreement, please visit the following link: www.seqrite.com/eula.

ALL MATTERS ARE SUBJECT TO PUNE (INDIA) JURISDICTION

Contents

Introduction 1

About Unified Threat Management (UTM) 1

Seqrite Terminator Features 1

Registration Wizard 3

License Agreement 4

Interface 4

DNS 6

Password Change 6

Date and Time 7

Product Key 8

Accessing Terminator 12

Logging in to Seqrite Terminator 12

Accessing Terminator through Web 12

Accessing Terminator through Command Line Interface (CLI) 13

Navigating through Seqrite Terminator (Web) 15

Dashboard 17

Notifications, Status & Internet Usage 17

Statistics area 20

Network Configuration 21

Definitions 21

Adding Definitions 21

Deleting Definitions 24

IPv6 24

Enabling IPV6 25

Enabling 6 to 4 tunnel 25

Interface 27

Configuring Interfaces 27

Deleting Interfaces 29

Adding Alias 30

USB Modem 31

DNS 33

Global DNS Server 33

Static DNS 35

Dynamic DNS 36

DHCP 37

Routing 41

Static Routing 41

Policy Based Routing (PBR) 42

Load Balance and Failover 47

Firewall 48

Default Firewall rules 49

Inter-zone Settings 50

Custom Firewall rules 51

IP Port Forwarding 55

VPN 57

Certificates 58

IPsec 61

PPTP VPN 65

SSL VPN 66

VLAN 74

Bridge 76

Link Aggregation 78

Internet Settings and Exclusion 80

Identity Management/ Users and Groups 83

User Management 84

Adding a user 84

Editing a User 86

Deleting users 87

Logging out a user by force 87

Importing users 88

Guest User Settings ... 89
Group Management ... 90
Adding a group ... 91
Edit Group ... 94
Deleting a group ... 94
Searching for groups ... 95
Time Category ... 95
Authentication Servers ... 96
Adding a new server ... 96
Importing/Deleting users from configured Authentication Servers ... 98
Delete Authentication servers ... 99
Synchronizing Seqrite Terminator with the Authentication servers ... 99
Scheduling synchronization of Seqrite Terminator with Authentication servers ... 100
Internet Quota ... 100
Content Filtering & Protection ... 104
Antivirus ... 105
Mail Protection ... 106
Global Settings ... 106
Antivirus ... 108
AntiSpam ... 109
Attachment Control ... 111
Keyword Blocking ... 113
URL Filtering ... 116
Category Based Web site blocking (URL Categorization) ... 116
White List ... 117
Blacklist (Customized Blocking) ... 118
MIME Filtering ... 119
Default MIME Filtering ... 119
Custom MIME Filtering ... 120
Keyword Blocking ... 121
Application Control ... 123

Intrusion Prevention System (IPS) 124
Default Rules 124
Custom Rules 125
Device Management 129
Administrator 129
Date and Time setting 129
Admin Settings 130
Adding Administrators 131
Admin Profiles 133
Web Portal Customization 135
SMTP Settings 136
Updates 138
Configuring Service Updates 138
Configuring System Updates 139
Configuring Manual Updates 140
Backup and Restore 143
Factory reset 147
License Details 148
Renew License 150
Enabling Seqrite Cloud 150
Logs and Reports 153
Internet Usage Report 153
Web site Access Report 155
Mail Protection Report 157
Web Protection Report 158
Intrusion Prevention Report 159
Policy Breach Attempts Report 160
Bandwidth Usage Report 161
Application Control Report 162
Firewall Reports 163
Updates 164

Log Viewer ... 165

Delete Report ... 167

Notification ... 169

Email notifications ... 169

SMS notifications ... 170

Add SMS Gateway ... 171

Edit SMS Gateway ... 173

Notification Configuration ... 173

Command Line Interface (CLI) ... 175

Configuring Seqrite Terminator using the CLI ... 175

Configure and manage Terminator ... 176

Web Management ... 177

Network Configuration ... 178

Managing Services using the CLI ... 180

Troubleshooting using the CLI ... 182

Troubleshooting Database Utilities ... 183

Troubleshooting Network Tools ... 184

Troubleshooting Debugging Information ... 184

Support ... 186

Troubleshooting ... 186

Email Support ... 187

Phone Support ... 187

Remote Support ... 187

Index ... 190

Chapter

1

Introduction

About 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. Unified Threat Management (UTM) is an integrated network security product that provides network administrators with all the security solutions in one device thus reducing the complexity.

This integrated solution helps administrator with single point of administration, monitoring and logging. It thus saves on the time and cost required to deploy and monitor multiple security solutions.

Seqrite Terminator Features

Seqrite Terminator is a UTM solution that combines various security solutions into a single security appliance. Seqrite Terminator 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	This is an additional paid feature. 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 (IPS)	Detects and prevents intrusion to protect your network. Protects your system from hackers who can sneak into the system.

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

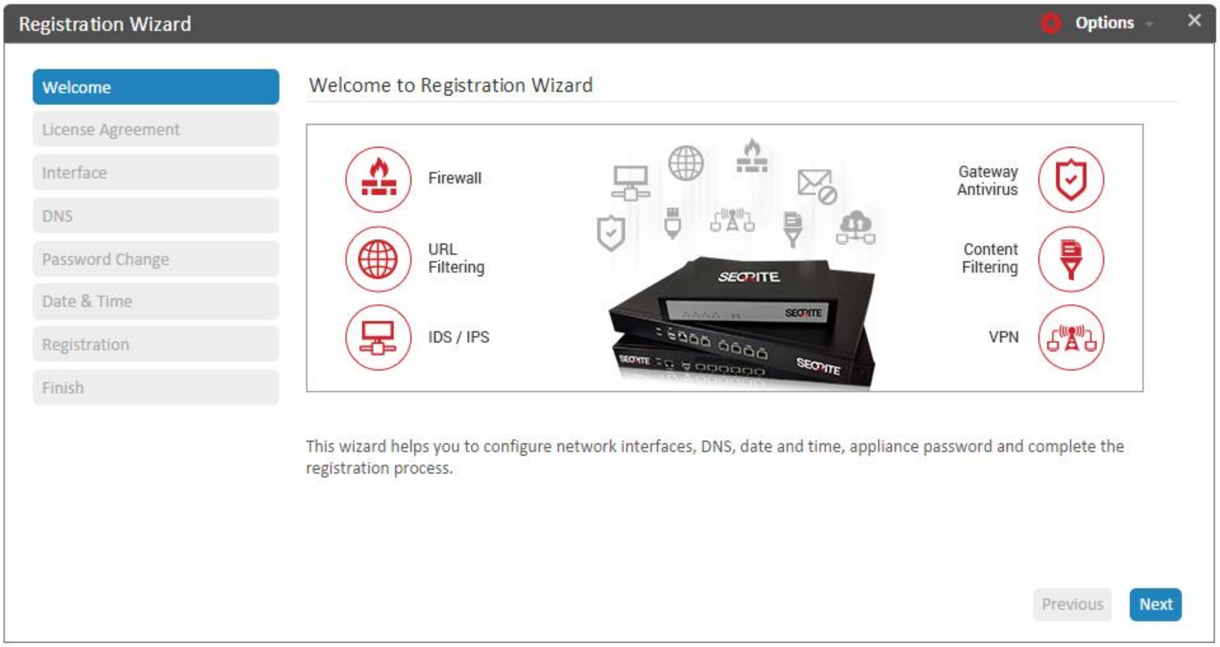
Features	**Description**
Gateway Mail Protection	Scans inbound and outbound email messages and email attachments. In-built spam filter runs a series of tests on inbound email messages. Terminator supports POP3, IMAP, and SMTP protocols.
Virtual Private Network (VPN)	Provides remote offices or roaming 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)	Terminator 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 Terminator. This feature allows traffic to be balanced across multiple ISP lines based on weightage and priority.
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 Terminator appliance requires license registration and network configuration prior to operation. On successful login through web interface of Terminator, 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.



This wizard helps you to configure network interfaces, DNS, date and time, appliance password and complete the registration process.

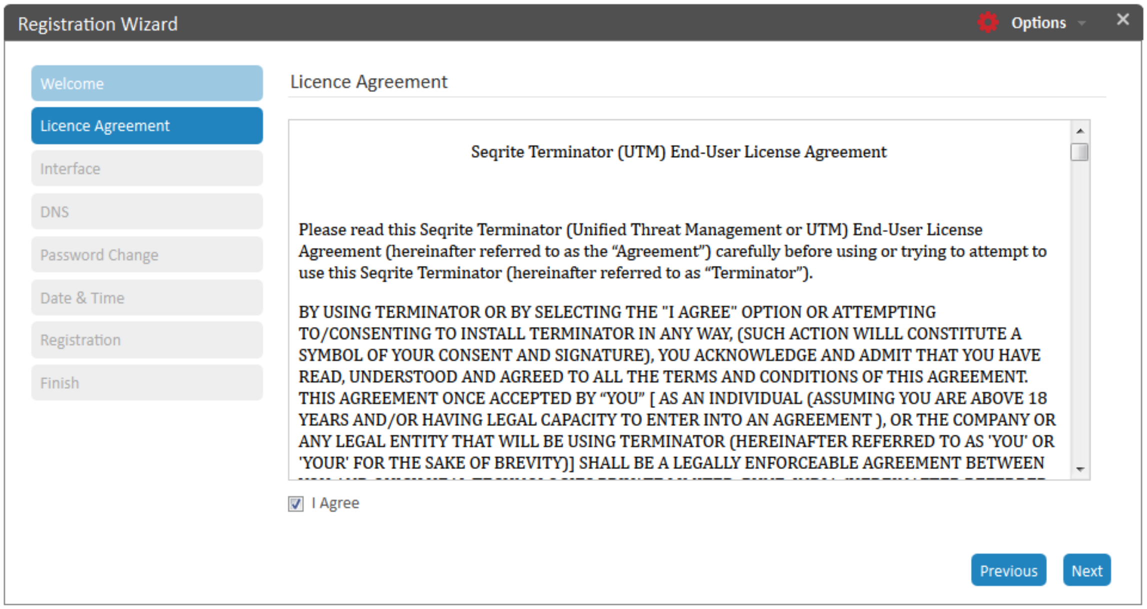
The Options button on the right side of the wizard provides the following options:

- Help: Provides a set of help files which guides you to use the Terminator.
- Shut down: Allows you to shut down the device.
- Restart: Allows you to restart the device.
- Logout: Allows you to log out of the device.
- System Information: Allows you to view system information.
- Diagnostic Tools: Allows you to collect debugging information of the different modules in Terminator.

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

License Agreement

The first step is to Agree to the User License agreement. On clicking the **Next** button on the welcome screen of the Registration Wizard, the User License Agreement appears. Read the License Agreement carefully and select the **I Agree** check box to accept the terms and conditions and then click **Next**.



Licence Agreement

Seqrite Terminator (UTM) End-User License Agreement

Please read this Seqrite Terminator (Unified Threat Management or UTM) End-User License Agreement (hereinafter referred to as the "Agreement") carefully before using or trying to attempt to use this Seqrite Terminator (hereinafter referred to as "Terminator").

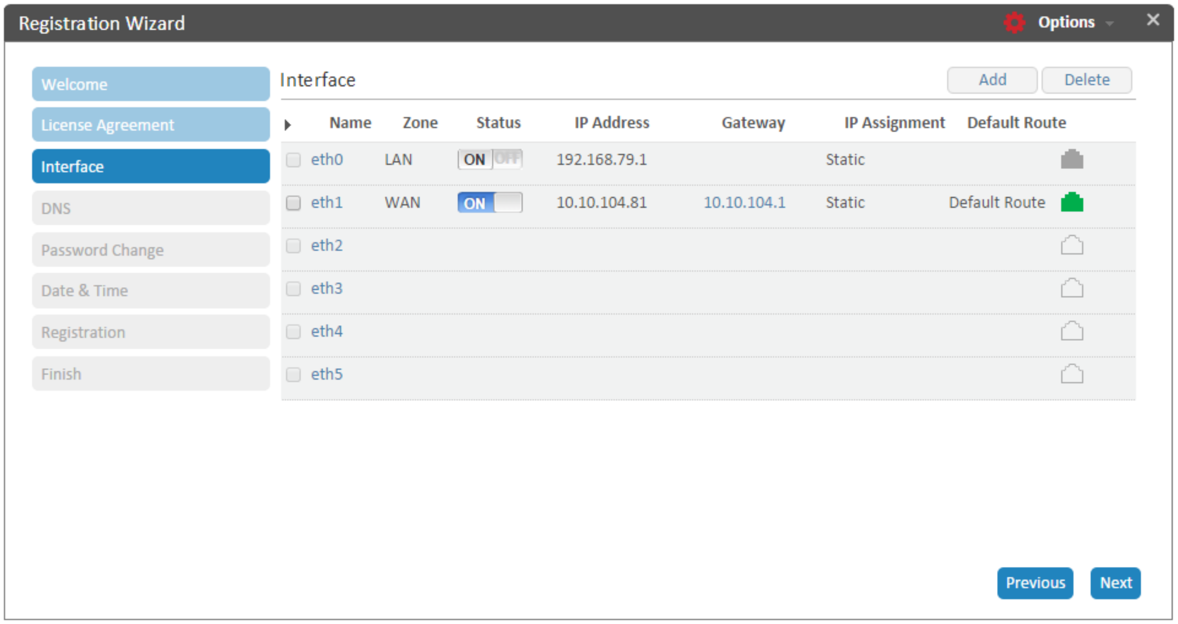
BY USING TERMINATOR OR BY SELECTING THE "I AGREE" OPTION OR ATTEMPTING TO/CONSENTING TO INSTALL TERMINATOR IN ANY WAY, (SUCH ACTION WILLL CONSTITUTE A SYMBOL OF YOUR CONSENT AND SIGNATURE), YOU ACKNOWLEDGE AND ADMIT THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. THIS AGREEMENT ONCE ACCEPTED BY "YOU" [AS AN INDIVIDUAL (ASSUMING YOU ARE ABOVE 18 YEARS AND/OR HAVING LEGAL CAPACITY TO ENTER INTO AN AGREEMENT), OR THE COMPANY OR ANY LEGAL ENTITY THAT WILL BE USING TERMINATOR (HEREINAFTER REFERRED TO AS 'YOU' OR 'YOUR' FOR THE SAKE OF BREVITY)] SHALL BE A LEGALLY ENFORCEABLE AGREEMENT BETWEEN

☑ I Agree

Interface

The next step is to configure the Interface settings in the Registration Wizard. On clicking the **Next** button on the User License Agreement screen, the Interface screen is displayed.

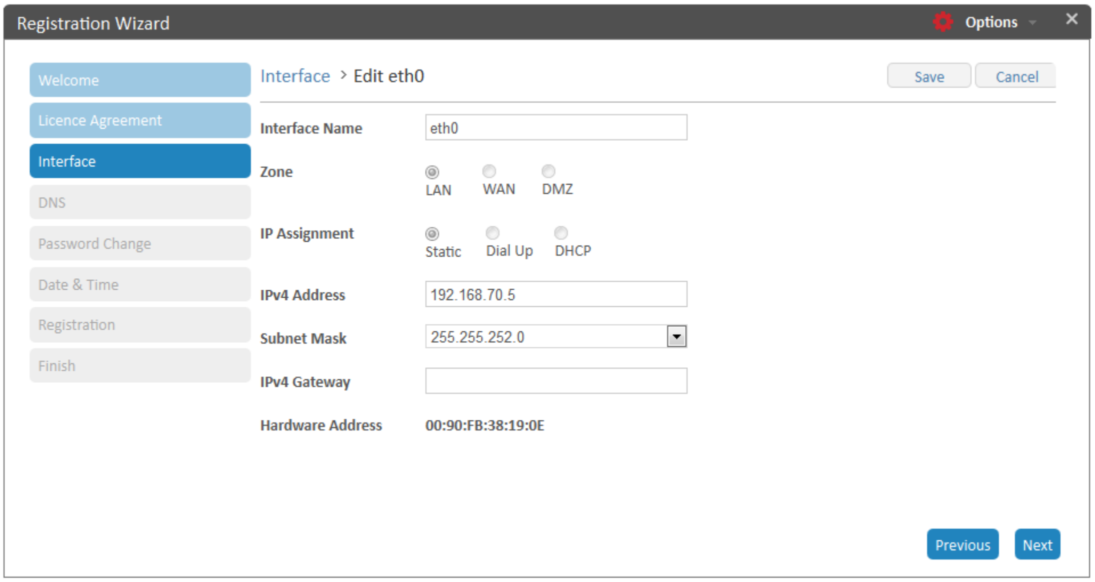
Note: The Interfaces with internet connectivity are indicated in green color.



Interface

Name	Zone	Status	IP Address	Gateway	IP Assignment	Default Route
eth0	LAN	ON	192.168.79.1		Static	
eth1	WAN	ON	10.10.104.81	10.10.104.1	Static	Default Route
eth2						
eth3						
eth4						
eth5						

1. To configure an interface, click the Name of the interface such as eth0 for LAN, eth1 for WAN.



Interface > Edit eth0

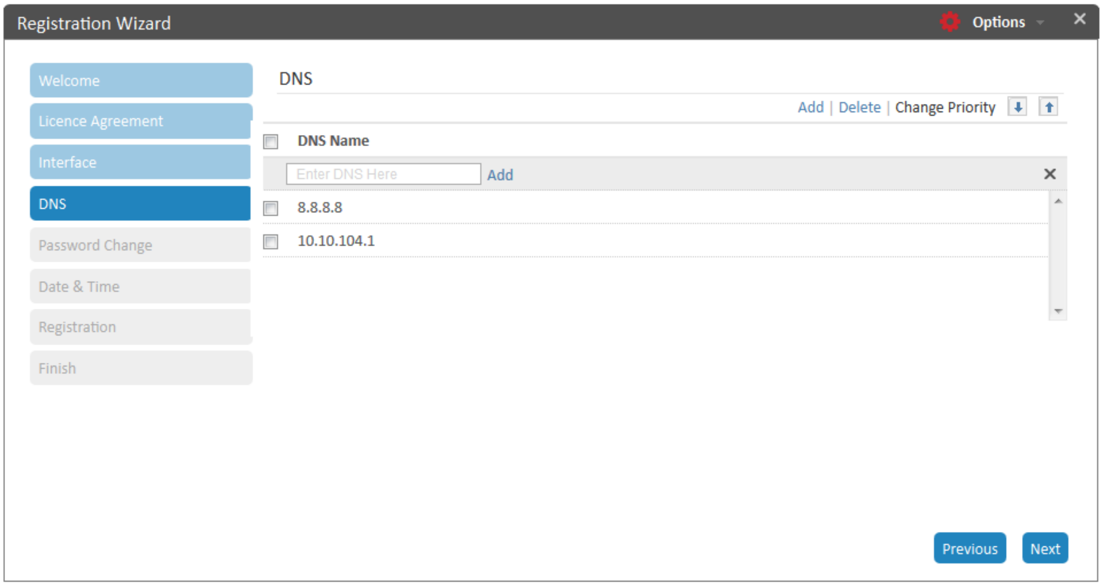
Interface Name	eth0
Zone	● LAN ○ WAN ○ DMZ
IP Assignment	● Static ○ Dial Up ○ DHCP
IPv4 Address	192.168.70.5
Subnet Mask	255.255.252.0
IPv4 Gateway	
Hardware Address	00:90:FB:38:19:0E

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, Dialup, or DHCP.
3. Click **Save** 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 Add interface see Interface section.)
5. Click **Next** to go to the next step that is DNS configuration.

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. You can also change the DNS priority, which allows you to try another DNS server if the current server is down.

1. Click **Add**.



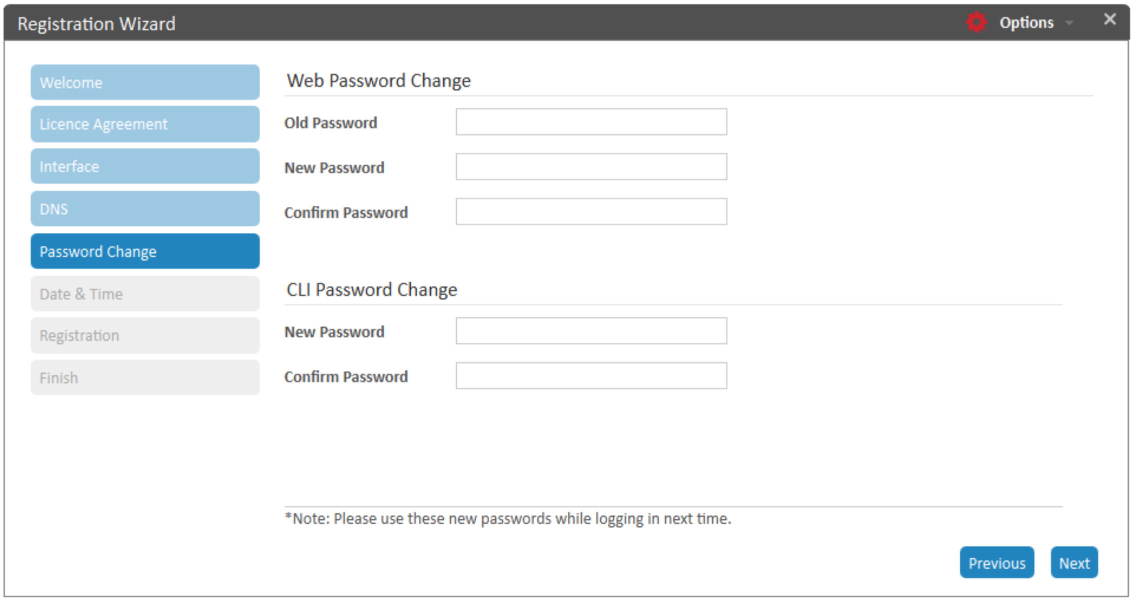
□	DNS Name
□	8.8.8.8
□	10.10.104.1

2. Enter **DNS Name** in the textbox and click **Add**. 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.

Password Change

You must change the default appliance password for web and CLI interface. On clicking the Next button in the DNS configuration screen the Password Change screen is displayed.

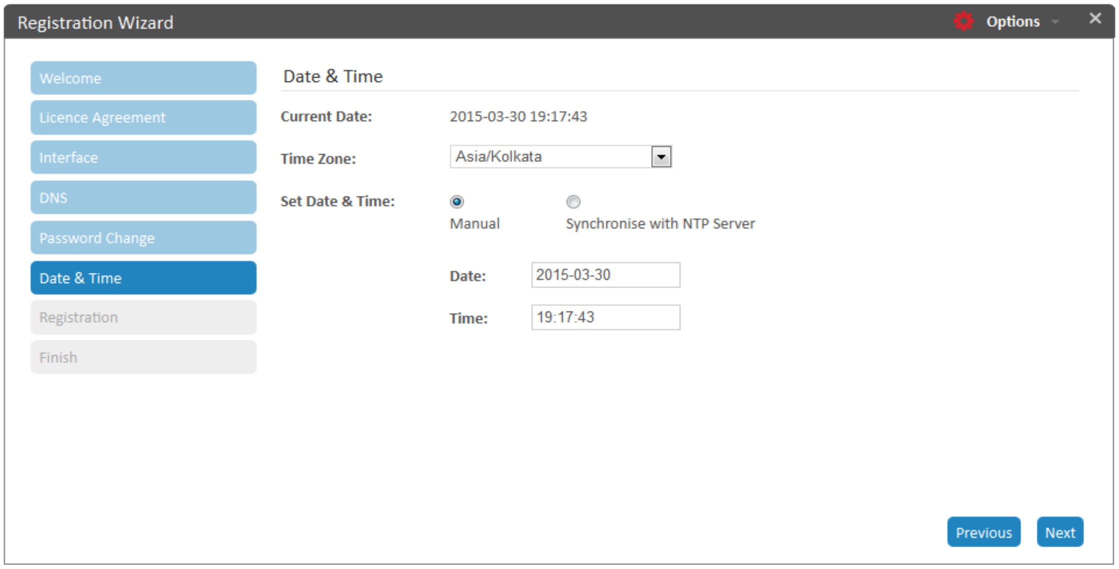


*Note: Please use these new passwords while logging in next time.

1. Set the new password for accessing Web and CLI interface.
2. Click **Next,** the new password will be saved**.** Next time you log in to the Web or CLI interface of Terminator you should use the new password.

Date and Time

After changing the password you need to configure the Date and time of the appliance. 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 appliance Date and Time as per different geographical regions. You can also synchronize the Date and time from an NTP server.



Current Date: 2015-03-30 19:17:43

Time Zone: Asia/Kolkata

Set Date & Time: ● Manual ○ Synchronise with NTP Server

Date: 2015-03-30

Time: 19:17:43

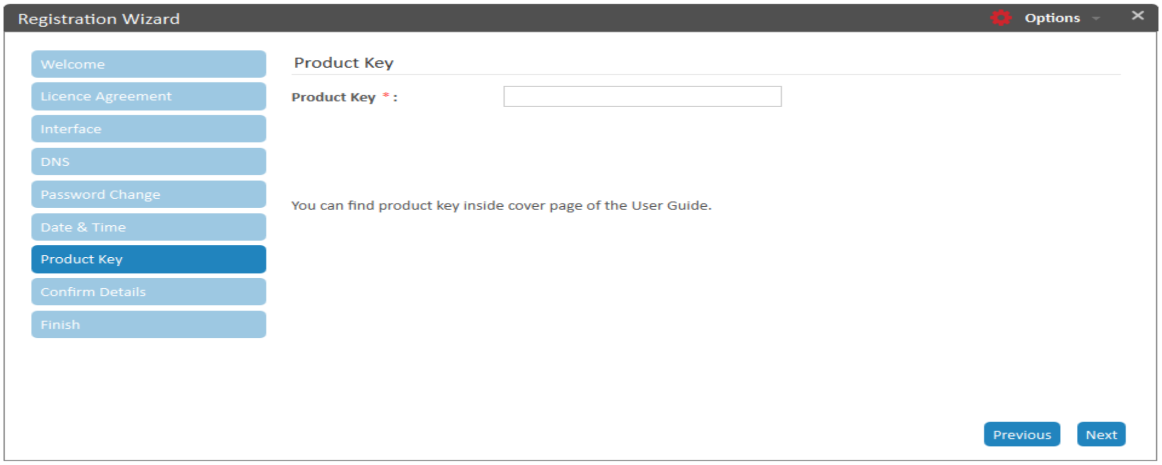
1. Select the **Time Zone** according to the geographical region in which the appliance is deployed.
2. Set **Date & Time** using one of the following two ways:
   - **Manual**: Select this option to set the date and time using the date and time pickers or
   - **Synchronize with NTP server**: Select 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.
3. Click **Next**.

Product Key

While registering the appliance you need to provide the Product key of your appliance. On clicking **Next** on the Date and Time setting screen, the Product Key screen is displayed.

1. Enter a valid Product Key and click **Next**. You can find product key inside cover page of the User Guide.

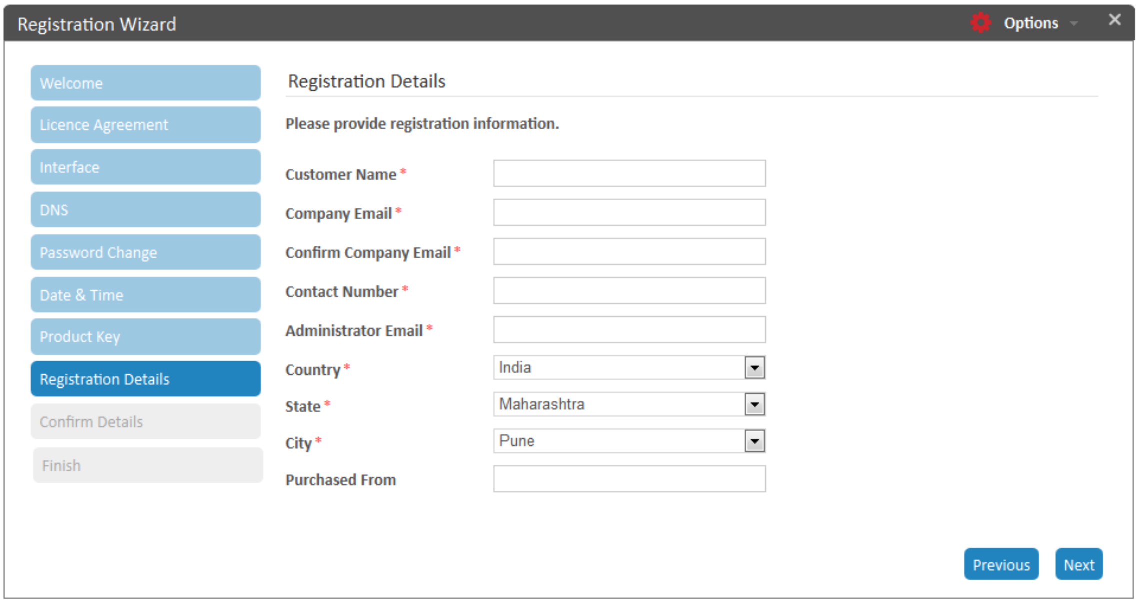


Product Key

Product Key * :

You can find product key inside cover page of the User Guide.

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



Registration Details

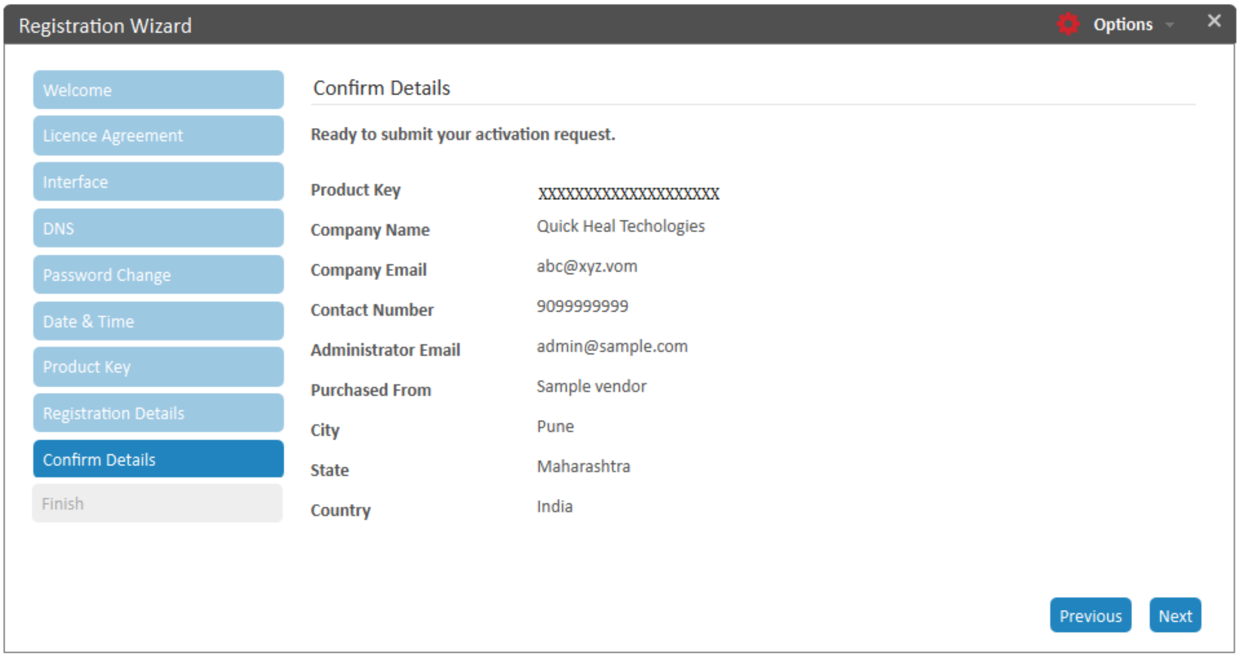
Please provide registration information.

Customer Name *	
Company Email *	
Confirm Company Email *	
Contact Number *	
Administrator Email *	
Country *	India
State *	Maharashtra
City *	Pune
Purchased From	

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

   Note: Fields marked with red asterisk are mandatory.

4. On clicking **Next**, the Confirm Details screen is displayed.

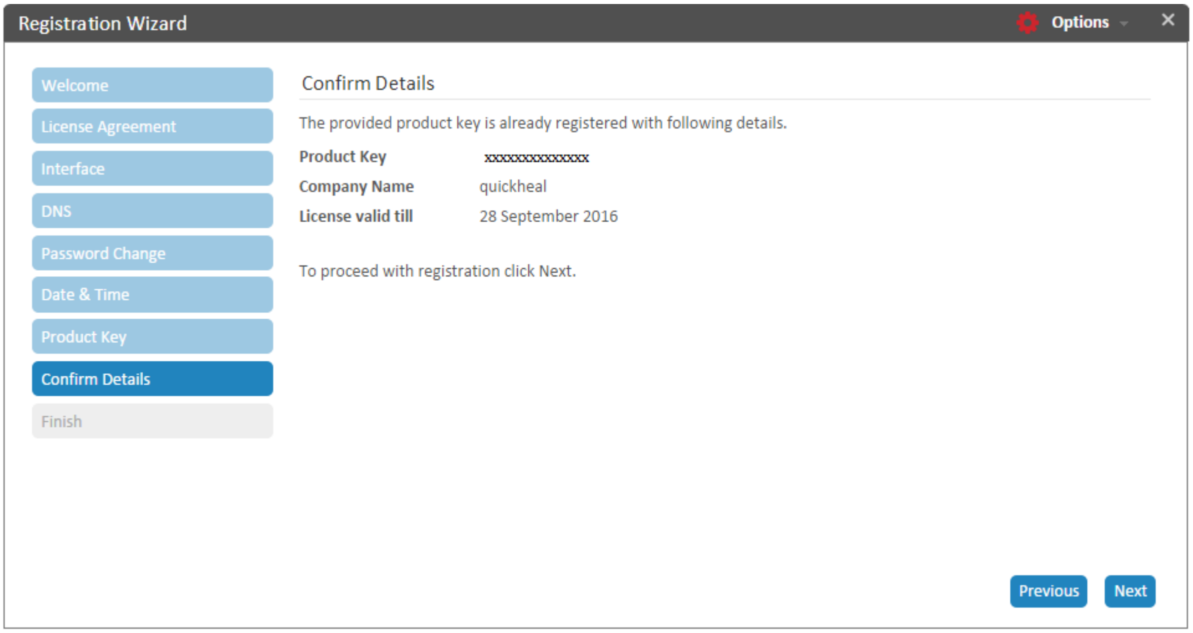


Confirm Details

Ready to submit your activation request.

Product Key	xxxxxxxxxxxxxxxxxxxx
Company Name	Quick Heal Techologies
Company Email	abc@xyz.vom
Contact Number	9099999999
Administrator Email	admin@sample.com
Purchased From	Sample vendor
City	Pune
State	Maharashtra
Country	India

5. If you upgrade the Terminator 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.



Confirm Details

The provided product key is already registered with following details.

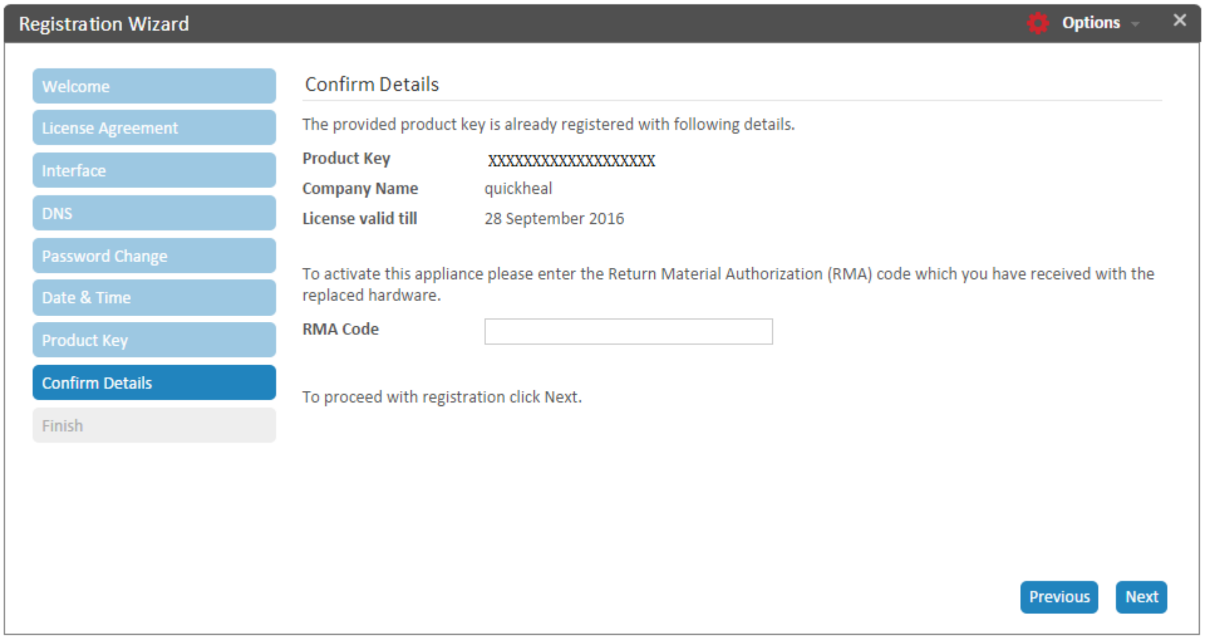
Product Key xxxxxxxxxxxxxxx

Company Name quickheal

License valid till 28 September 2016

To proceed with registration click Next.

6. Confirm the details and click **Next.**
7. 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.



Confirm Details

The provided product key is already registered with following details.

Product Key XXXXXXXXXXXXXXXXXXX

Company Name quickheal

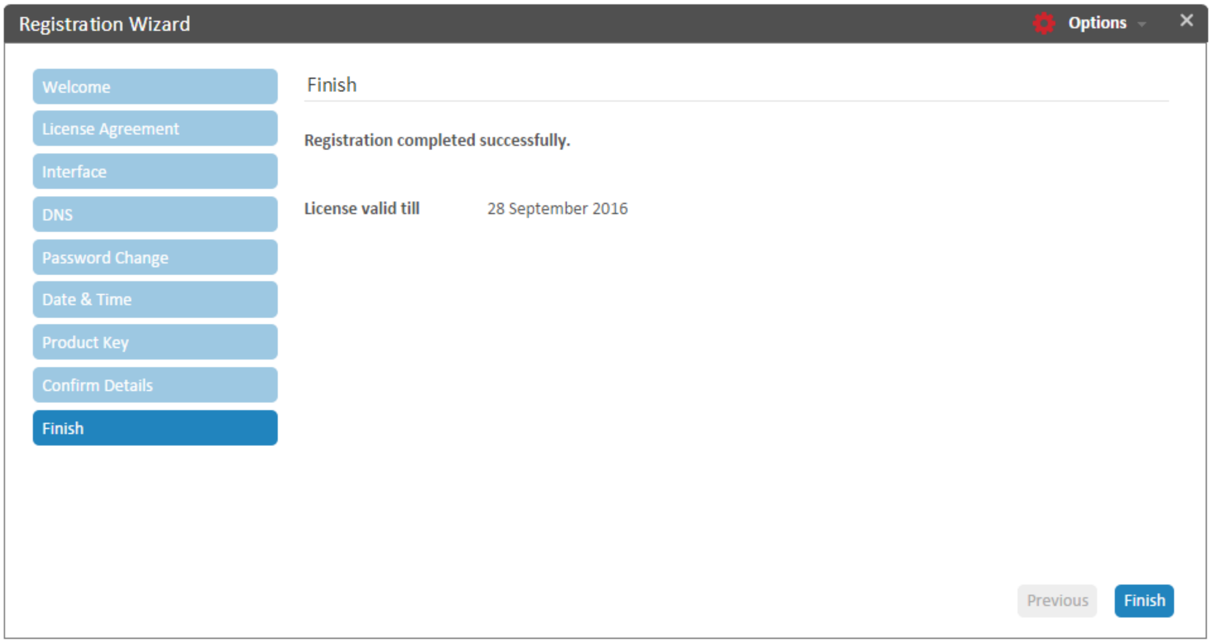
License valid till 28 September 2016

To activate this appliance please enter the Return Material Authorization (RMA) code which you have received with the replaced hardware.

RMA Code

To proceed with registration click Next.

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



Finish

Registration completed successfully.

License valid till 28 September 2016

10. Click **Finish**, to finish the registration process of the appliance. On clicking **Finish**, you will be logged out. Login again using the new password.

    For more details on how to use the features and other relevant information, refer to the Help section of Seqrite Terminator.

    For additional technical support, consult the Seqrite Terminator technical support center.

Chapter

3

Accessing Terminator

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 Terminator you can refer the Seqrite Terminator Getting Started Guide or Seqrite Terminator Cookbook.

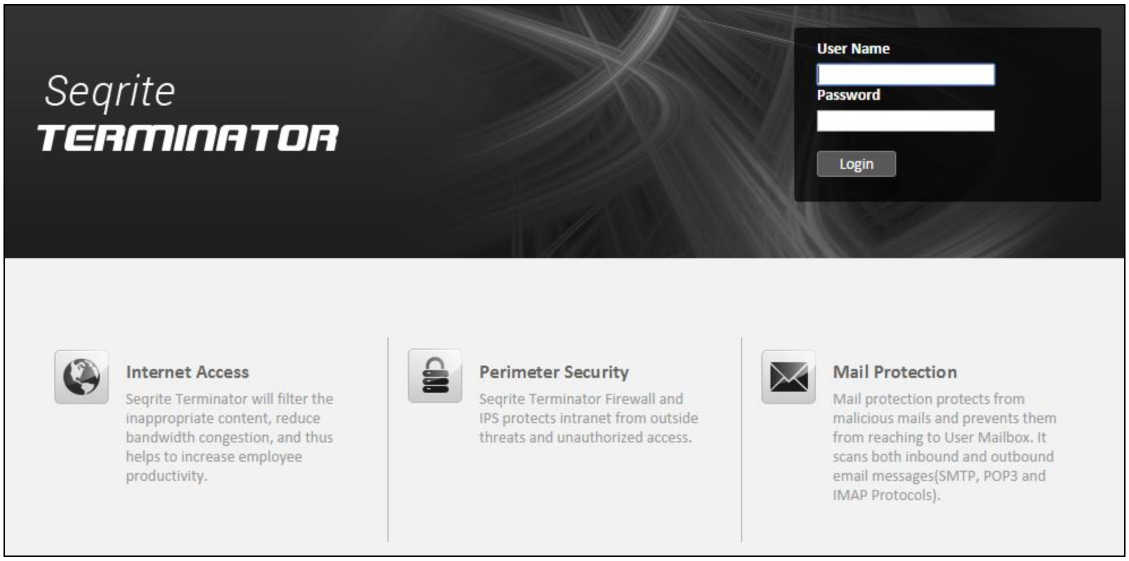
Logging in to Seqrite Terminator

You can use the following two ways to access Terminator:

- Accessing Terminator through Web
- Accessing Terminator through CLI

Accessing Terminator through Web

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



Internet Access
Seqrite Terminator will filter the inappropriate content, reduce bandwidth congestion, and thus helps to increase employee productivity.

Perimeter Security
Seqrite Terminator Firewall and IPS protects intranet from outside threats and unauthorized access.

Mail Protection
Mail protection protects from malicious mails and prevents them from reaching to User Mailbox. It scans both inbound and outbound email messages(SMTP, POP3 and IMAP Protocols).

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

Accessing Terminator through Command Line Interface (CLI)

Apart from using the web interface to login to the Seqrite Terminator, you can login to the Seqrite Terminator 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 Terminator components.

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

Username: admin

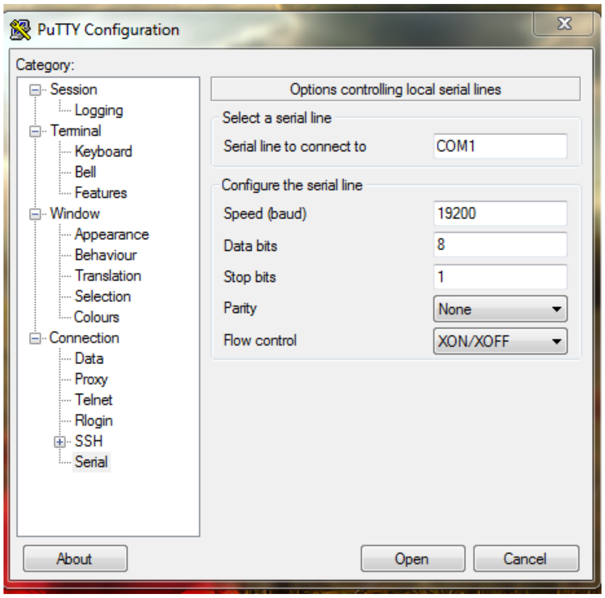
Password: admin@123

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

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

  When you connect the Terminator using a console cable, make the following settings in putty, to access CLI.

  - Set the speed baud rate as 19200.



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 19200

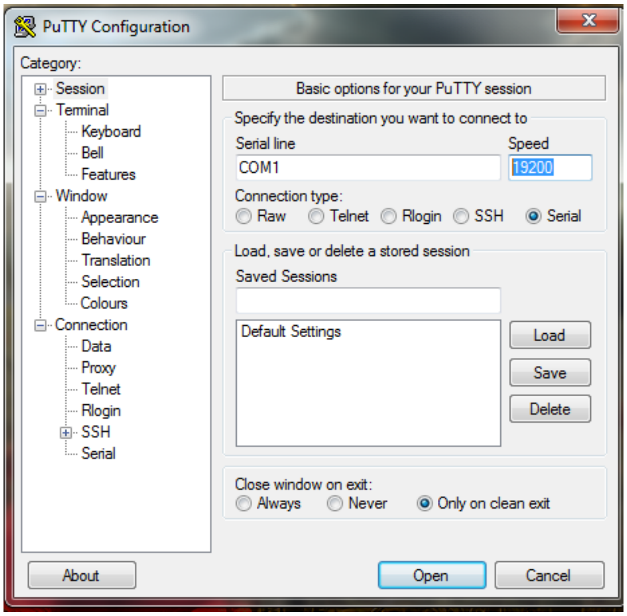
Data bits: 8

Stop bits: 1

Parity: None

Flow control: XON/XOFF

  - Select the Connection type as Serial, as shown below:

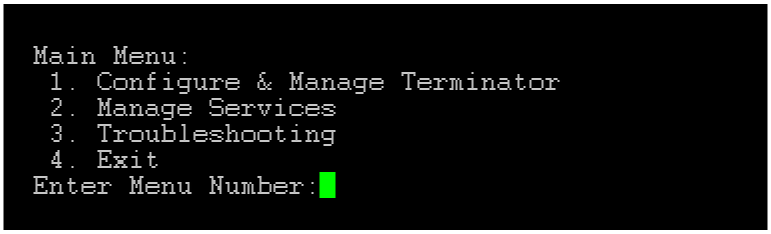


Serial line: COM1
Speed: 19200
Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial
Saved Sessions: Default Settings
Close window on exit: ○ Always ○ Never ● Only on clean exit

- **Remote connection**: You can remotely connect to the Seqrite Terminator in the following ways:
    - Accessing CLI console via remote login utility.
    - Telnet xxx.xxx.xxx.xxx where xxx.xxx.xxx.xxx is the IP address of the Terminator server.

      Note: Telnet is disabled by default.
    - Accessing CLI console using SSH client. You can access Seqrite Terminator CLI console using a SSH client.

      Note: SSHv1 and SSHv2 both are supported.
- On successful login, the following Main Menu screen will be shown:



```
Main Menu:
 1. Configure & Manage Terminator
 2. Manage Services
 3. Troubleshooting
 4. Exit
Enter Menu Number:
```

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.

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

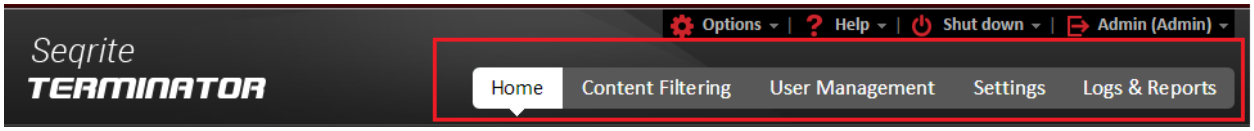
1. **Configure and manage terminator**: Helps you to reset web Super Administrator password, configure interfaces & DNS, reboot and shut down the Terminator appliance.

2. **Troubleshooting**: Helps you to Ping & Traceroute IP.

Navigating through Seqrite Terminator (Web)

Accessing the Seqrite Terminator through a web based console is easy to use and has the features and options grouped according to the category.

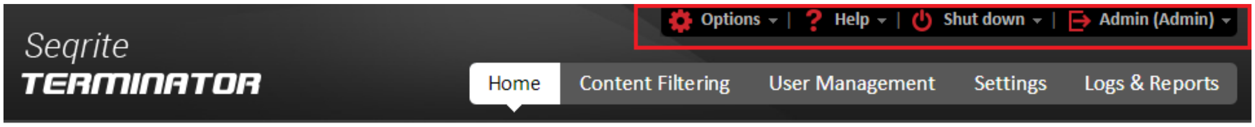
The user interface on the Seqrite Terminator is divided into the following 5 main sections as shown in the figure below:



- **Home** - Provides basic summary of the Seqrite Terminator features and various usage graphs.
- **Content Filtering** - Allows configuration of content filtering like content blocking, Web site blocking, customized blocking and whitelisting.
- **User Management** - Allows configuration of Users, Guest Users, Groups, Time Category details and Authentication server.
- **Settings** - Allows configuration of various settings for Seqrite Terminator. It includes the Internet settings, mail server settings, firewall, interface settings, VLAN, VPN etc.
- **Logs and Reports** - Provides reports regarding Internet Usage, Website Access, Virus Protection, Policy Breaches etc.

Common options

The uppermost part of the User Interface has the following options that are common to all of the tabs and can be used from any of the pages.



Tab	Function
Options	**Change web password** – To change the user password. Use Change Web Password to change the password of the currently logged in administrator. On clicking this the following options are displayed **Old Password**: Provide the current password of the logged in administrator. **New Password**: Provide the new password which should be set. **Confirm Password**: Re-enter the new password. On clicking **Submit**, the password is changed and administrator is logged out. Administrator should login with new password.

Tab	Function
	Note: Even if you change the Web password of super administrator the CLI password is not changed. **Reset CLI password** – To reset the CLI password. The CLI can be accessed by super administrator user. The password for CLI access can be changed using this option. On clicking this the following options are displayed. **New Password**: Provide the new CLI password which should be set. **Confirm Password**: Confirm the new password. On clicking **Submit**, the CLI password is changed. **SSL certificate** – To download SSL certificate. Seqrite Terminator uses a self-signed certificate. The certificate will be downloaded in .der format.
Help	**Help** – Provides a set of help files which guides you to use the Terminator. **License Info** – For viewing the current license information. **Support** – For accessing the available support options.
Shut down	Allows you to shut down or restart the device.
Admin	Displays the name of the logged in user and the profile type whether Read-only or Admin mode. If the profile type is Admin, then that user has write access that is the user can make changes and save the configurations. User with Read Only access cannot make any changes to the configurations. **Logout**: Allows you to log out of the device.

Chapter

4

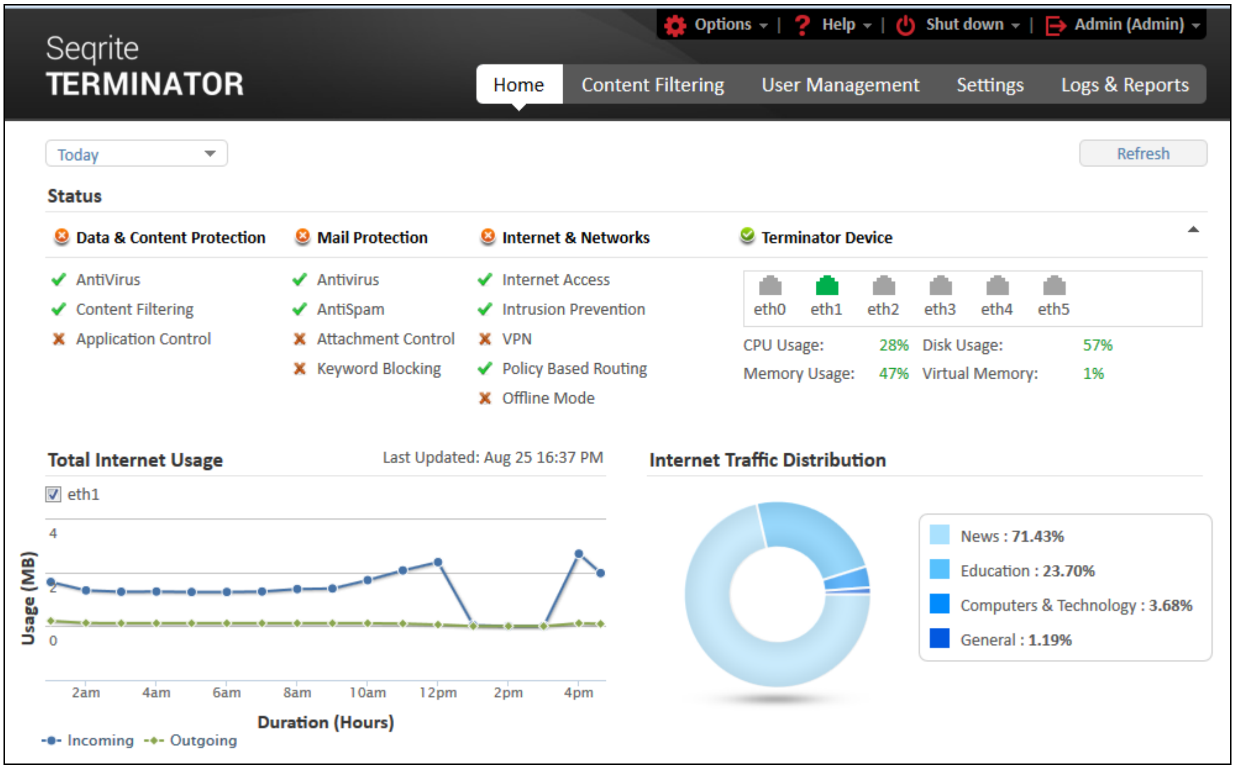
Dashboard

The Home page or the dashboard is the first page that is displayed when you log in to Seqrite Terminator. The dashboard displays the real-time status of the various activities carried out by the Seqrite Terminator. The data on home page can be updated to latest value by using **Refresh** button.

The dashboard on the Home page is made up of the following two parts which you can access by scrolling down or up as required:

- Notifications, Status and Internet usage area
- Statistics area

Notifications, Status & Internet Usage



Status

Data & Content Protection
- ✓ AntiVirus
- ✓ Content Filtering
- ✗ Application Control

Mail Protection
- ✓ Antivirus
- ✓ AntiSpam
- ✗ Attachment Control
- ✗ Keyword Blocking

Internet & Networks
- ✓ Internet Access
- ✓ Intrusion Prevention
- ✗ VPN
- ✓ Policy Based Routing
- ✗ Offline Mode

Terminator Device

eth0 eth1 eth2 eth3 eth4 eth5

CPU Usage: 28% Disk Usage: 57%

Memory Usage: 47% Virtual Memory: 1%

Total Internet Usage Last Updated: Aug 25 16:37 PM

☑ eth1

Internet Traffic Distribution

- News : 71.43%
- Education : 23.70%
- Computers & Technology : 3.68%
- General : 1.19%

- **Notifications area** – Displays the alerts and notifications for the following:
  - If number of licenses has exceeded

- License has expired
- Antivirus protection out of date
- If Update Service is not running

The following table explains the scenarios and describes when the notifications are displayed.

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 Terminator are more than or equal to the licensed users limit.
Update service is not running. Please contact technical support.	This notification is displayed when the Antivirus database update service has stopped running.
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 Terminator 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 Terminator. 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 gets 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 Terminator license has expired. Please renew your license.	This notification is displayed when the Terminator license has already expired. When the Terminator License expires the Antivirus Update and Web site categorization services are stopped. Once 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.

Notification	Description
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. The logs are deleted from the archive if the logs reach the limit. The oldest log is deleted first.
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.

You also get an option to update and resolve the issue. There can be multiple notifications in parallel depending on the number of warnings made by the application.

- **Status area** – Displays the current status of the various settings for data and content protection, mails, Internet and networks, and whether the protection is activated or not.

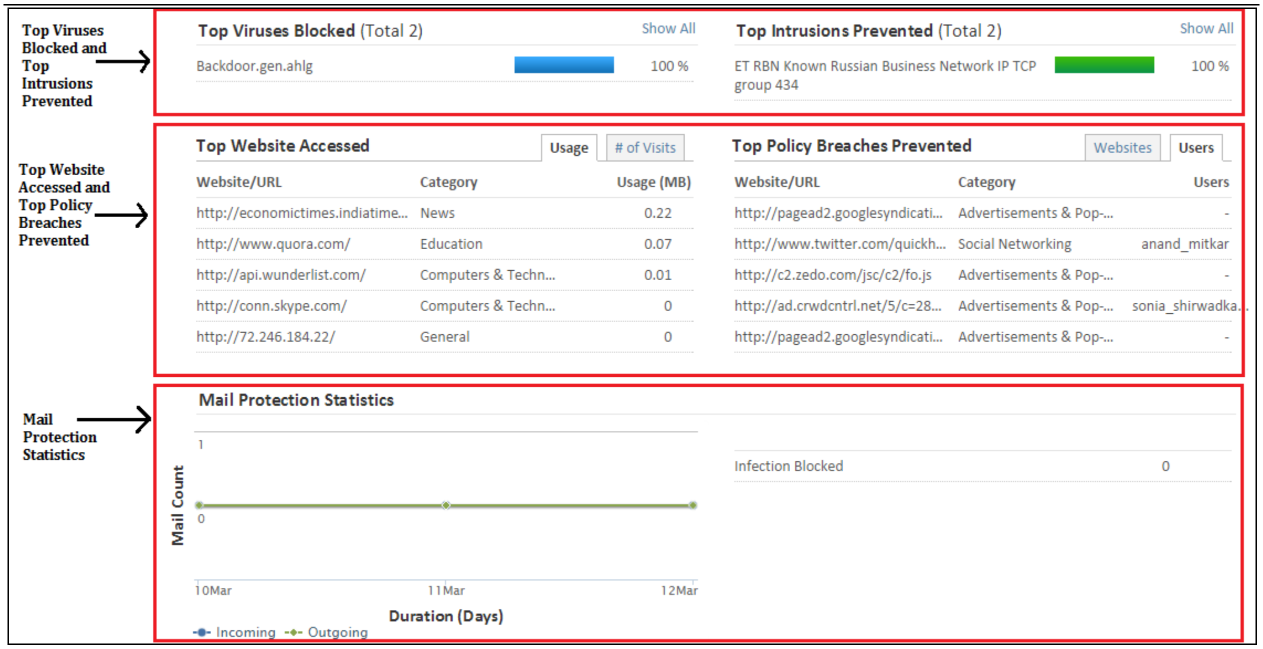
Status	Description
✓	Indicates module is enabled and running.
✗	Indicates module is disabled or module is enabled but not running.

- **Terminator Device –** In this section the status of various Ethernet ports of Terminator device is shown. The CPU Usage, Disk Usage, Memory Usage, and Virtual memory status in real time is also displayed.

Icon	Description
■	Indicates that Ethernet cable is connected.
🟩	Indicates that the Ethernet cable is connected & Internet is available.
□	Indicates that Ethernet cable is not connected.

- **Total Internet Usage and Internet Traffic distribution** – Displays the total Internet usage for incoming and outgoing traffic and the breakup percentage-wise for Internet access by content category.

Statistics area


Top Viruses Blocked and Top Intrusions Prevented
Top Website Accessed and Top Policy Breaches Prevented
Mail Protection Statistics
Show All
Show All
Usage
# of Visits
Websites
Users
Mail Count
1
0
10Mar
11Mar
12Mar
Duration (Days)
Incoming
Outgoing

Top Viruses Blocked (Total 2)

Backdoor.gen.ahlg	100 %

Top Intrusions Prevented (Total 2)

ET RBN Known Russian Business Network IP TCP group 434	100 %

Top Website Accessed

Website/URL	Category	Usage (MB)
http://economictimes.indiatime...	News	0.22
http://www.quora.com/	Education	0.07
http://api.wunderlist.com/	Computers & Techn...	0.01
http://conn.skype.com/	Computers & Techn...	0
http://72.246.184.22/	General	0

Top Policy Breaches Prevented

Website/URL	Category	Users
http://pagead2.googlesyndicati...	Advertisements & Pop-...	-
http://www.twitter.com/quickh...	Social Networking	anand_mitkar
http://c2.zedo.com/jsc/c2/fo.js	Advertisements & Pop-...	-
http://ad.crwdcntrl.net/5/c=28...	Advertisements & Pop-...	sonia_shirwadka...
http://pagead2.googlesyndicati...	Advertisements & Pop-...	-

Mail Protection Statistics

Infection Blocked	0

- **Top Viruses Blocked and Top intrusions Prevented** – Displays the top viruses that Seqrite Terminator has blocked, and the top intrusion activities that were prevented from affecting the network.

- **Top websites Accessed and Top Policy Breaches** – Displays the top Web sites accessed by name, and the number of visits. It also displays the number of attempts to access the blocked URLs. The Users tab displays the list of the users who have tried to access the blocked URLS.

- **Mail Protection Statistics** – Displays the scan statistics for incoming and outgoing mail.

- **Infection Blocked –** Displays the number of mails blocked that have infected attachments.

  Note: You can view the above statistics for a period of last 24 hours, last week or last month by selecting the drop-down option on the top of the Notifications areas.

Chapter

5

Network Configuration

Definitions

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

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

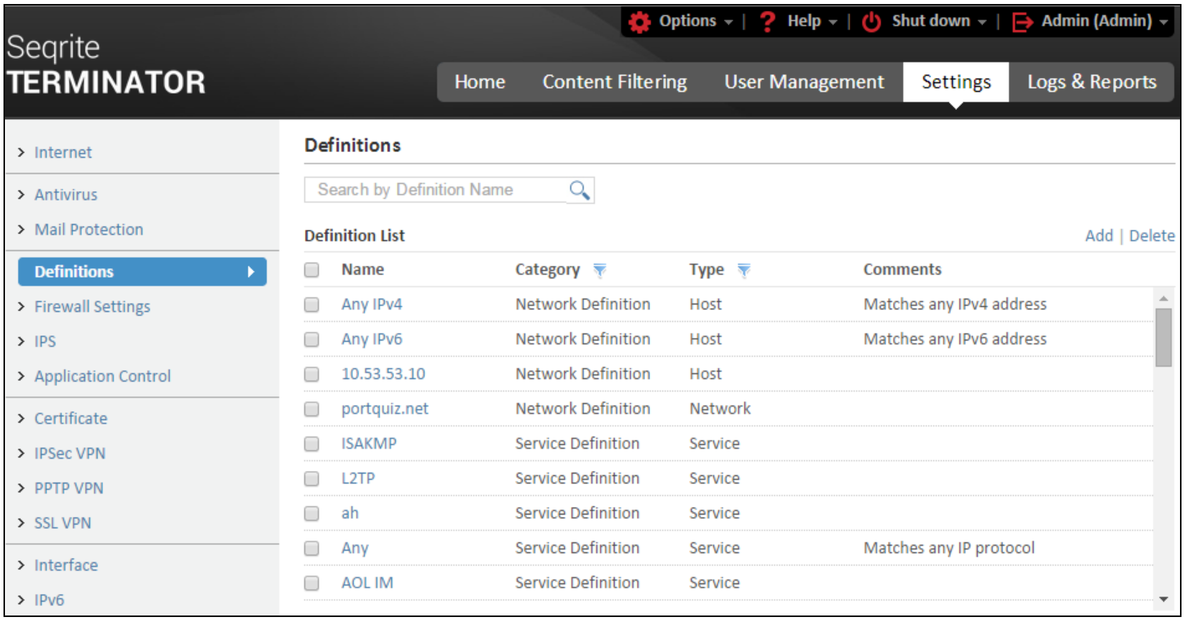
Service definition: Helps you to add protocols and ports used by an application for communication.

The Definition 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 Definitions

To add a Network definition follow the steps given below:

1. Log on to **Seqrite Terminator > Settings > Definition**. The following page is displayed:

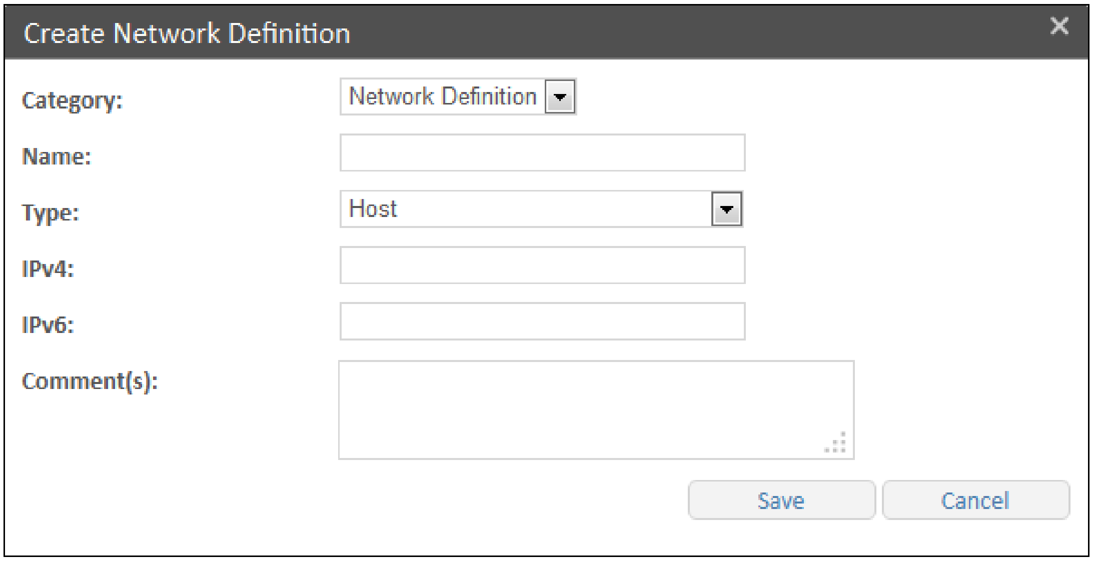


Definitions

Definition List

□	Name	Category	Type	Comments
□	Any IPv4	Network Definition	Host	Matches any IPv4 address
□	Any IPv6	Network Definition	Host	Matches any IPv6 address
□	10.53.53.10	Network Definition	Host	
□	portquiz.net	Network Definition	Network	
□	ISAKMP	Service Definition	Service	
□	L2TP	Service Definition	Service	
□	ah	Service Definition	Service	
□	Any	Service Definition	Service	Matches any IP protocol
□	AOL IM	Service Definition	Service	

2. Click **Add**. The Add Network Definition dialog box is displayed.



Create Network Definition

Category: Network Definition

Name:

Type: Host

IPv4:

IPv6:

Comment(s):

3. Select the **Category** as Network Definition.
4. Enter the definition name in **Name.**
5. **Type**: This option is displayed if you select the **Network Definition** category.

   Network definitions are of the following four types.

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

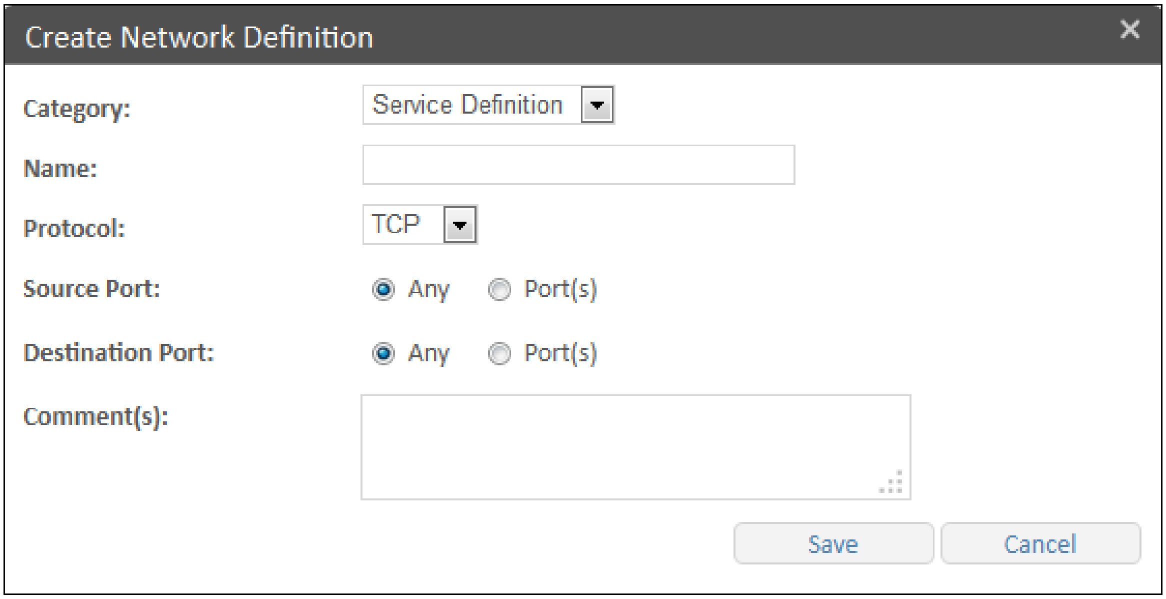
   ii. **IP Range**: Allows you to define sequence of IP addresses. Enter IPv4 /IPv6 address range.

   iii. **IP List**: Allows you to define random list of IP address. Enter comma separated list of IPv4 / IPv6 IP address (es).

   iv. **Network**: Allows you to define a network containing a set of IP addresses. Enter IPv4 network address and select subnet mask from dropdown. For IPv6 enter IPv6 network address and IPv6 prefix value.
6. Enter the description for the definition in the **Comments** textbox.
7. Click **Save**. The newly added Network definition is displayed in the list on the Definitions page.

To add a Service definition follow the steps given below:

1. Log on to **Seqrite Terminator > Settings > Definition**.
2. Click **Add**. The Add Network Definition dialog box is displayed.
3. Select **Category** as Service Definition.



Create Network Definition

Category: Service Definition

Name:

Protocol: TCP

Source Port: ● Any ○ Port(s)

Destination Port: ● Any ○ Port(s)

Comment(s):

4. Enter the Service definition **Name**.

5. **Protocol**: This option is displayed when you choose **Service Definition c**ategory. Select the protocol from dropdown. The protocol are of the following 4 types:

   i. TCP

   ii. UDP

   iii. ICMP

   iv. IGMP

6. **Source Port:** This option is displayed when you choose Service definition Category. Select an option for Source port. 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 single port or a range of ports.

7. **Destination Port:** This option is displayed when you choose Service definition Category. Select an option for Destination port. 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.

8. **Comments**: Enter the description for the service definition.

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

Deleting Definitions

To delete a Definition follow the steps given below:

1. Log on to **Seqrite Terminator> Settings > Definition**. The following page is displayed:
2. Select the Definitions that you want to delete and click **Delete**.

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

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

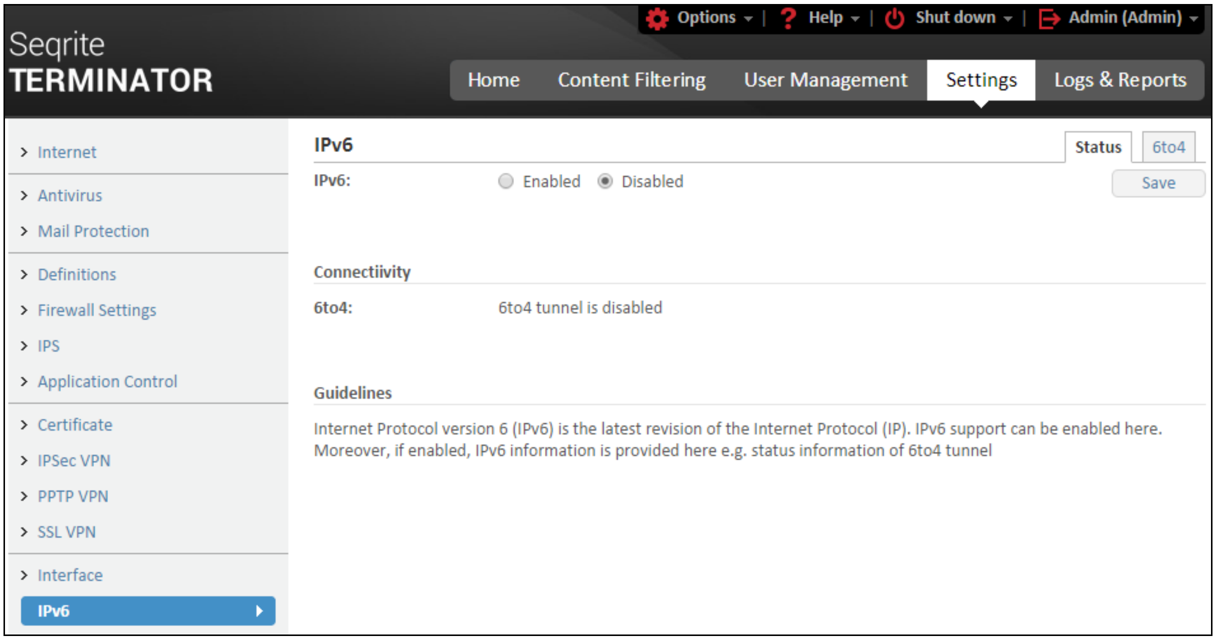
- Interface
- DNS
- DHCP
- Content Filtering (Blacklist / whitelist and Domain)

Seqrite Terminator 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

To enable IPV6 follow the steps given below:

1. Log on to Seqrite Terminator**> Settings > IPv6**. By default IPv6 support is disabled.



IPv6

IPv6: ○ Enabled ● Disabled

Connectiivity

6to4: 6to4 tunnel is disabled

Guidelines

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP). IPv6 support can be enabled here. Moreover, if enabled, IPv6 information is provided here e.g. status information of 6to4 tunnel

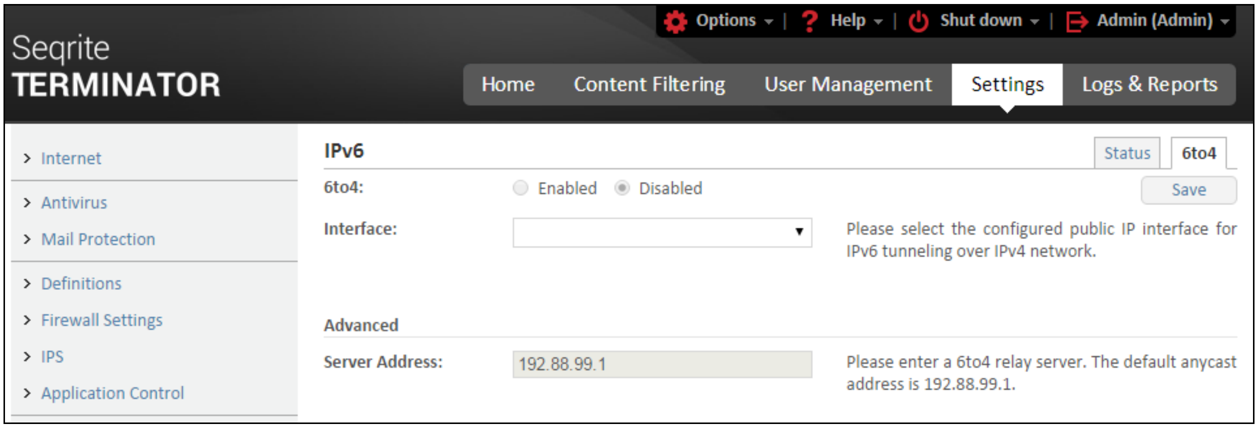
2. Select **Enable** and click **Save**.

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

Enabling 6 to 4 tunnel

To enable IP address tunneling for a certain interface, follow the steps given below:

1. Log on to Seqrite Terminator**> Settings > IPv6**.
2. Click **6 to 4**. The following page is displayed.



IPv6

6to4: ○ Enabled ● Disabled

Interface: Please select the configured public IP interface for IPv6 tunneling over IPv4 network.

Advanced

Server Address: 192.88.99.1 Please enter a 6to4 relay server. The default anycast address is 192.88.99.1.

3. Select **Enabled** 6to4 tunnel.
4. Select an **Interface.** This Interface should be of a public WAN with IPv4 address and on which 6to4 tunnel is to be created.
5. Enter **Server Address** in the **Advanced** section. This option helps to set the relay server, you can either set it or use the default 192.88.99.1 as relay server.

Interface

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

Terminator 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 Terminator 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 Terminator 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

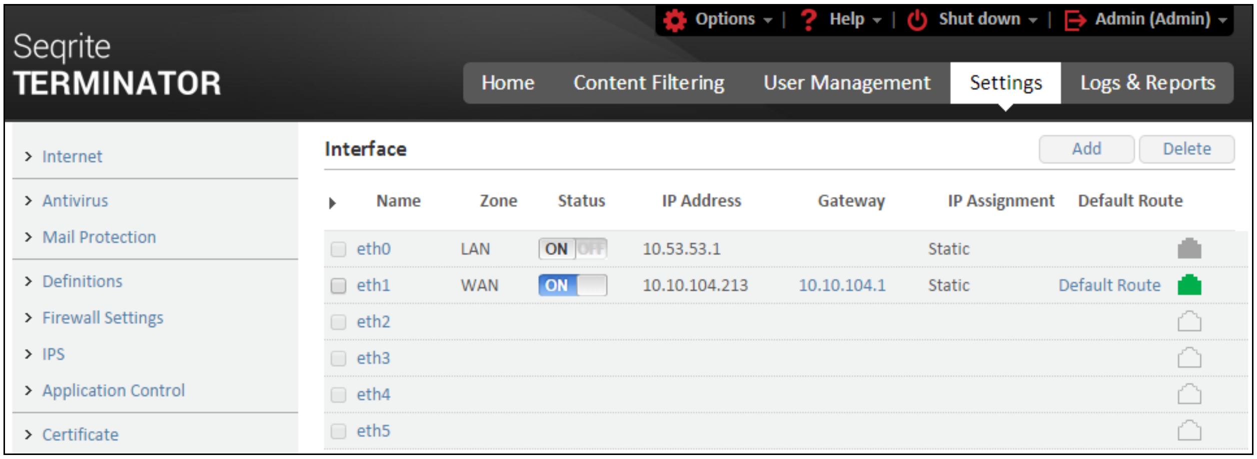
The Interface page initially displays the list of all the default interfaces. These interfaces are the ports on the Terminator appliance. The Alias and VLAN interface that are added under the default ports are displayed in the interface list as a sub-interface of the base interface.

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

Icon	Description
■	Ethernet cable is plugged in.
🟩	Ethernet cable is plugged in and Internet is available.
🟩□	Ethernet cable is not connected for all slaves, Internet is available (Link Aggregation).
■□	Ethernet cable is not connected for all slaves (Link Aggregation).
□	Ethernet cable is not plugged.

To configure a physical interface follow these steps:

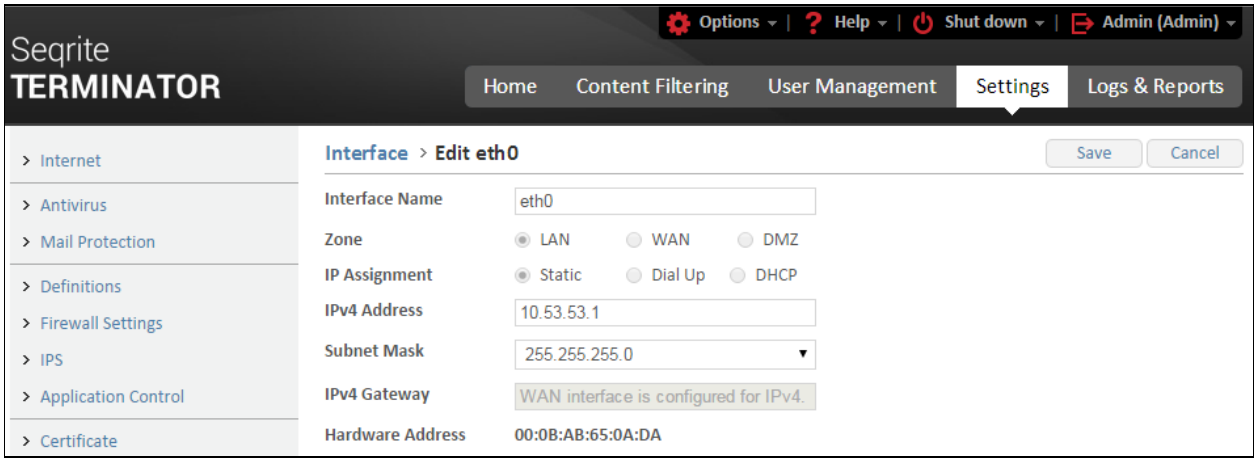
1. Log on to **Seqrite Terminator > Settings > Interfaces**. The Interfaces list is displayed.



Interface

Name	Zone	Status	IP Address	Gateway	IP Assignment	Default Route
□ eth0	LAN	ON	10.53.53.1		Static	
□ eth1	WAN	ON	10.10.104.213	10.10.104.1	Static	Default Route
□ eth2						
□ eth3						
□ eth4						
□ eth5						

2. Click the interface name in the list. The following page is displayed.



Interface > Edit eth0

Interface Name	eth0
Zone	● LAN ○ WAN ○ DMZ
IP Assignment	● Static ○ Dial Up ○ DHCP
IPv4 Address	10.53.53.1
Subnet Mask	255.255.255.0 ▾
IPv4 Gateway	WAN interface is configured for IPv4.
Hardware Address	00:0B:AB:65:0A:DA

The table explains the fields on the page:

Field	Description
Interface Name	Set the name of Interface.
Zone	Select from LAN, WAN, and DMZ.
IP assignment	This can be Static, Dial up, or DHCP. i. If you select the IP assignment as Static then you need to enter the IPV4 address and Subnet mask. ii. If you select the IP assignment as Dialup then you need to enter the user name and password provided by your ISP.
IPv4 Address	This field is displayed if you select IP assignment as Static. Set IPv4 address for the Seqrite Terminator, through which all clients will access

Field	Description
	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 Terminator 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.
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.

3. Click **Save**.

Deleting Interfaces

To delete an Interface, follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > Interfaces**. The Interfaces list is displayed.
2. Select the Interface that you want to delete and click **Delete**. A confirmation message is displayed.
3. Click **OK** to confirm deletion of the interface.

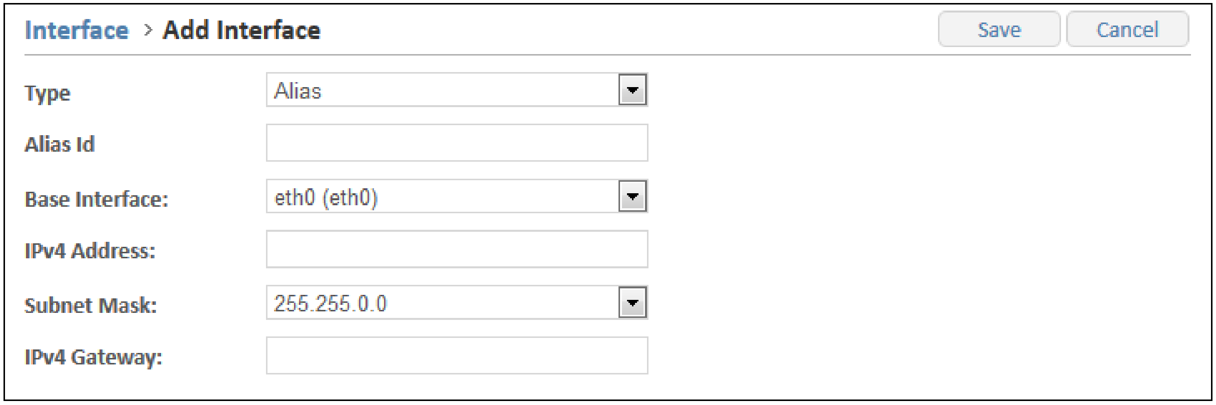
   Note: You cannot delete interface eth0. Deleting the interfaces will only clear the configuration / settings, the port will still be displayed in the list.

Adding Alias

Adding an Alias interface allows you to configure multiple IP addresses to a single interface / port. Adding Alias feature gives the base interface another identity. The zone of base interface is the zone of Alias.

To add an Alias follow the steps given below:

1. Log on to Seqrite Terminator**> Settings> Interface**. The Interface details page is displayed.
2. Click **Add**. The following page is displayed.
3. Select the **Type** of Interface as **Alias**.



Type	Alias
Alias Id	
Base Interface:	eth0 (eth0)
IPv4 Address:	
Subnet Mask:	255.255.0.0
IPv4 Gateway:	

4. Enter the following details:

   i. **Alias Id**: This is a unique number used to identify the Alias.

   ii. Select the **Base Interface**. You can use only the configured interfaces.

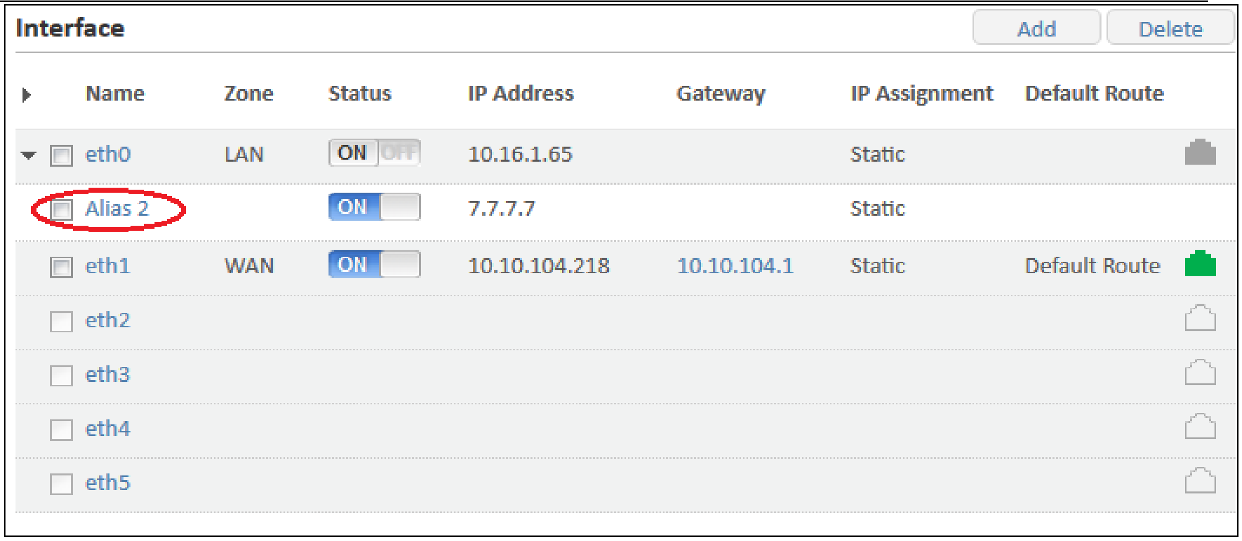
   iii. Enter the **IPv4** IP address.

   iv. Enter the **Subnet mask**.

   v. Enter the **IPV4 gateway** address.

5. Click **Save**.

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



Interface

Name	Zone	Status	IP Address	Gateway	IP Assignment	Default Route
eth0	LAN	ON OFF	10.16.1.65		Static	
Alias 2		ON	7.7.7.7		Static	
eth1	WAN	ON	10.10.104.218	10.10.104.1	Static	Default Route
eth2						
eth3						
eth4						
eth5						

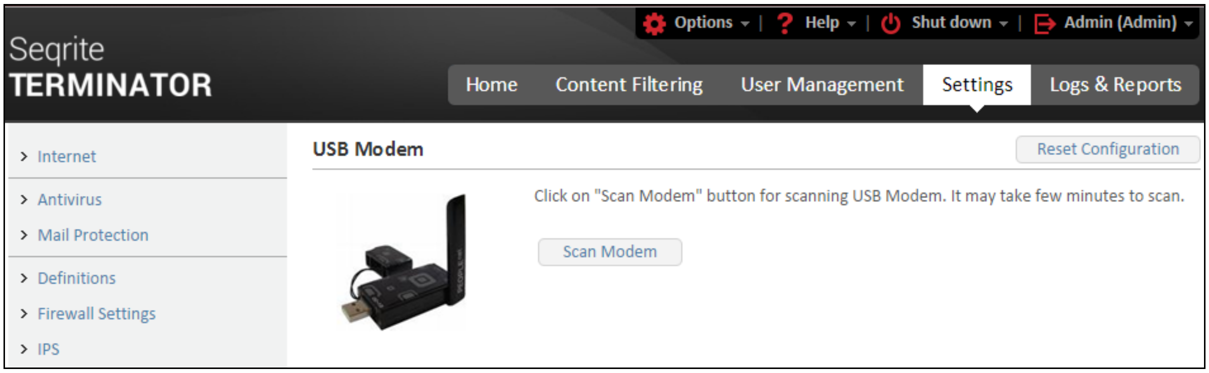
USB Modem

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

To configure a USB modem, follow the steps given below:

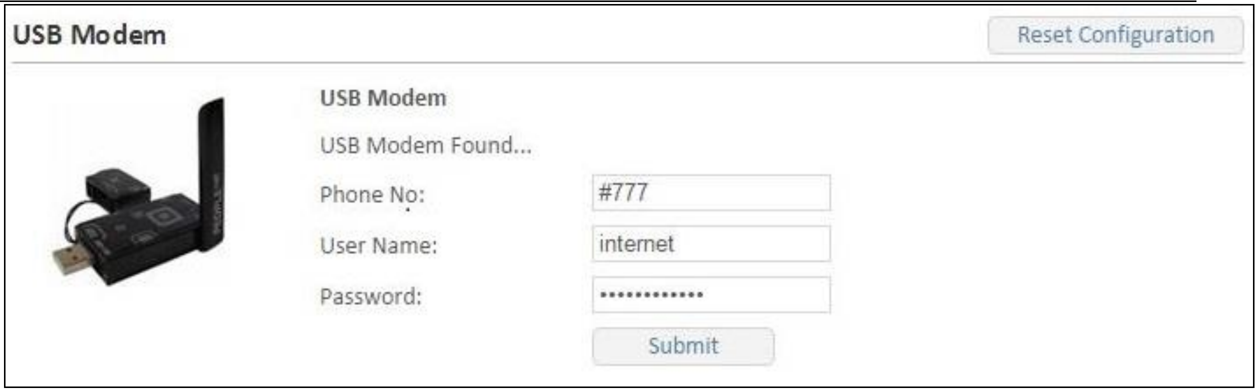
1. Log on to Seqrite Terminator **> Settings> USB Modem**. The USB Modem page is displayed with the Scan Modem and Reset configuration buttons.



USB Modem

Click on "Scan Modem" button for scanning USB Modem. It may take few minutes to scan.

2. Click **Scan Modem**. The Terminator scans and detects the USB modem and displays the configuration options.



USB Modem

USB Modem Found...

Phone No: #777

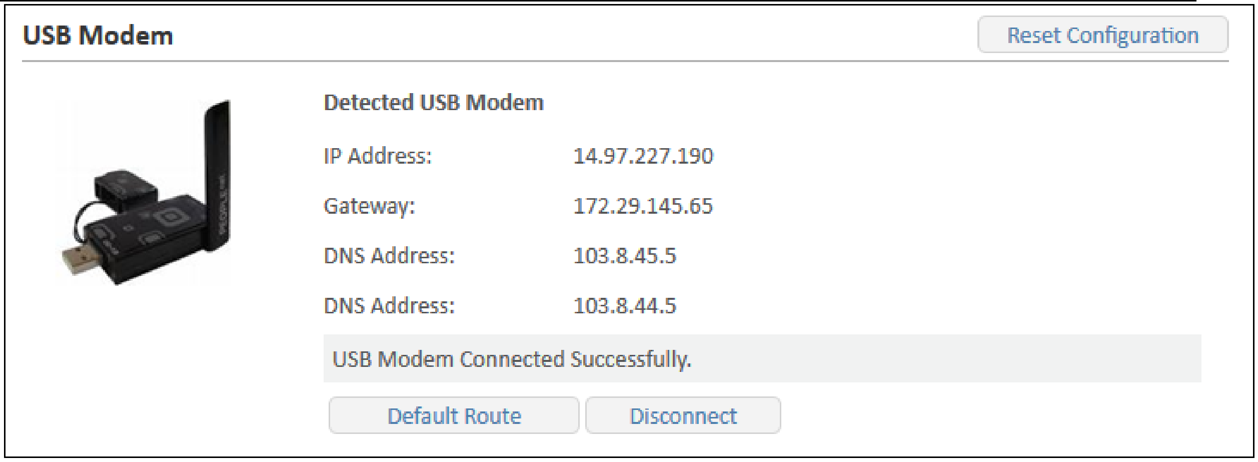
User Name: internet

Password: •••••••••••••

3. Enter the following details and click **Submit**:

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.

4. On clicking **Submit**, the USB will be connected the details for the detected modem are displayed:



Detected USB Modem

IP Address: 14.97.227.190

Gateway: 172.29.145.65

DNS Address: 103.8.45.5

DNS Address: 103.8.44.5

USB Modem Connected Successfully.

5. You can use the following options as required:

- Set the detected USB modem as Default Route.

- Disconnect the USB.
- Reset Configuration if the USB.

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.

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 Terminator 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 Terminator to try to use another DNS server in case the server you are using is unavailable.

Seqrite Terminator supports the following types of DNS configurations:

- Static DNS
- Dynamic DNS

Global DNS Server

Using the Global 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.

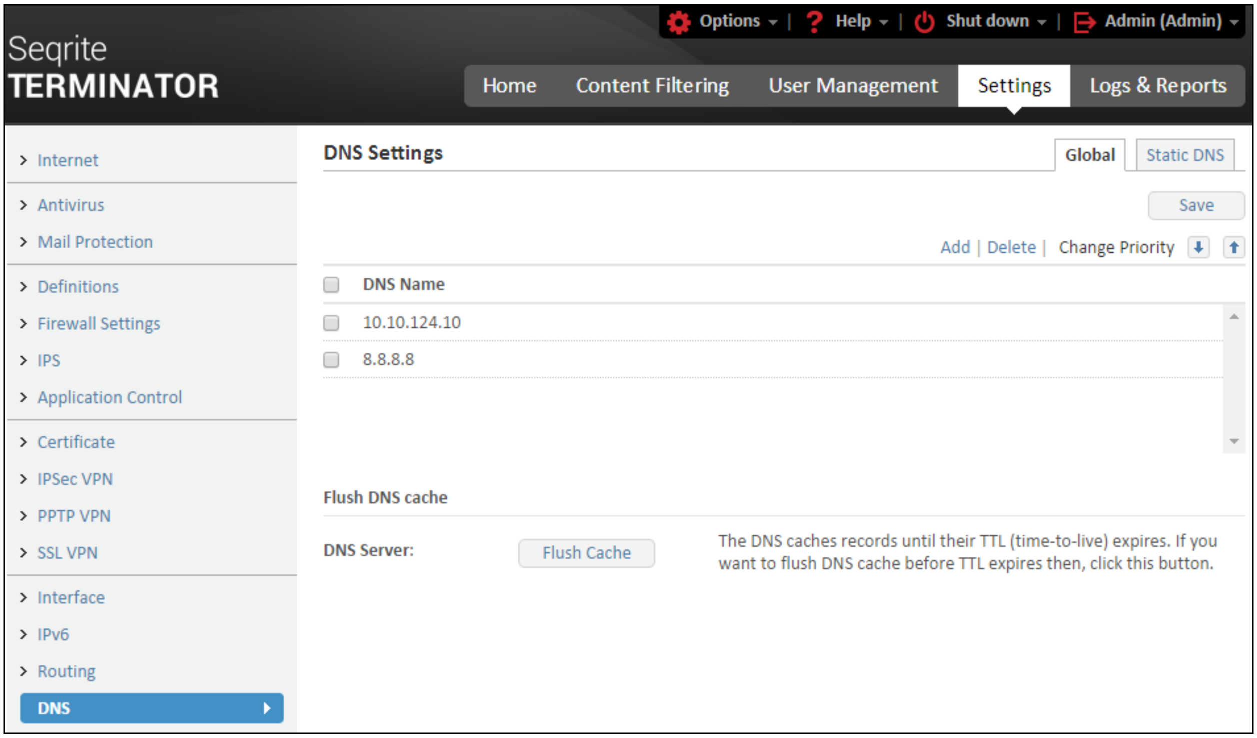
Note: You can add IPv6 DNS only if you have enabled the IPv6 feature on Seqrite Terminator. For more details on IPV6 feature see **IPv6**.

By default the DNS with IP address 8.8.8.8 is used.

Adding a Global DNS servers

To add a Global DNS server, follow the steps given below:

1. Log on to Seqrite Terminator**> Settings> DNS**. The DNS Settings page is displayed which contains the list of DNS servers.



DNS Name
10.10.124.10
8.8.8.8

The DNS caches records until their TTL (time-to-live) expires. If you want to flush DNS cache before TTL expires then, click this button.

2. Click **Add.** Enter the IP address of the DNS in the designated textbox and click **Add**.

Deleting Global DNS servers

To delete a Global DNS server, follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > DNS**. The DNS Settings page is displayed which displays the list of DNS servers.
2. Select the server you want to delete and click **Delete**. You can select and delete multiple servers at the same time.

Changing Priority

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.

To change priority of the DNS Server follow the steps given below:

1. Log on to Seqrite Terminator**> Settings > DNS**. The DNS Settings page is displayed with the list of DNS servers.

2. Select the required DNS server and click the arrow buttons to move the DNS server names up or down as per the priority.

Flush DNS Cache

The DNS uses a cache to temporarily store the IP address records. Each of these record 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.

To empty the DNS cache, follow the steps given below:

1. Log on to Seqrite Terminator**> Settings > DNS**. The DNS Settings page is displayed which displays the list of DNS servers.
2. Click **Flush Cache.** The cache is flushed and contents are deleted.

Static DNS

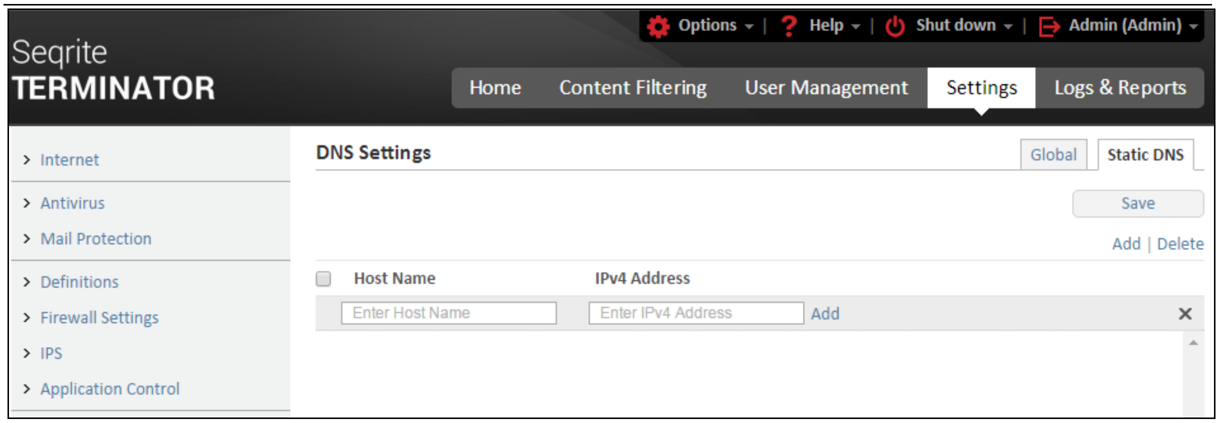
If you know the IP address of a host, then you can add a static DNS entry for the hosts in Terminator. Whenever you access this host, the Terminator will resolve and return the added IP address.

Using the Static DNS section you can add and delete Static DNS.

Adding Static DNS entry

To add a Static DNS entry follow the steps given below:

1. Log on to Seqrite Terminator**> Settings> DNS**. The DNS Settings page is displayed with a list of DNS servers. The Global DNS list is displayed by default.
2. Click **Static DNS** on the upper-right side to display the Static DNS page.



3. Click **Add** to add a new DNS entry. Enter the Host Name and IPv4 address, in the designated textboxes.
4. Click **Save**.

Deleting Static DNS Entry

To delete a Static DNS entry, follow the steps given below:

1. Log on to Seqrite Terminator**> Settings> DNS** on the left pane. The DNS Settings page is displayed which displays the list of DNS servers. The Global DNS list is displayed by default.
2. Click **Static DNS** on the upper-right side to display the Static DNS page. Select the host you want to delete and click **Delete**. You can also select and delete multiple Static DNS hosts at a time.

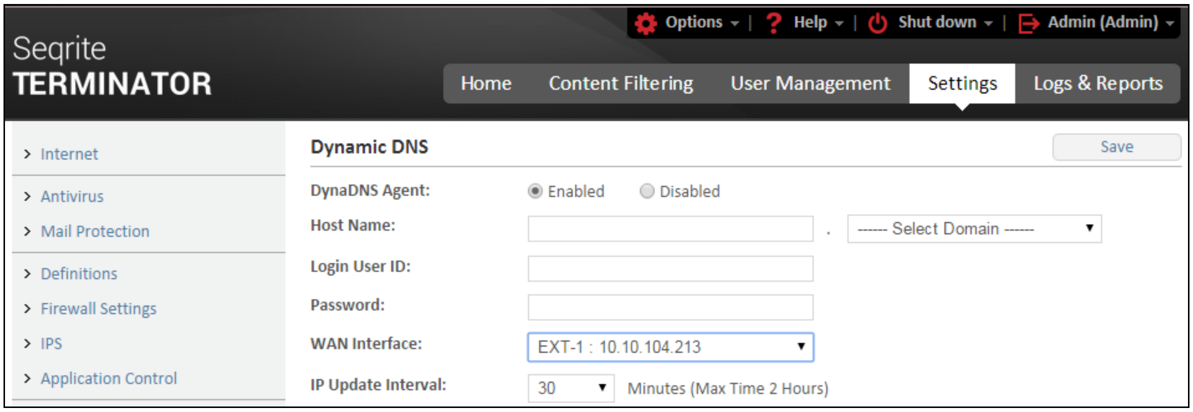
Dynamic DNS

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 changed 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 Terminator allows you to configure the DDNS account that you have purchased from the DDNS service provider and bind it to a WAN interface.

To configure DDNS in Terminator follow the steps given below:

1. Log on to Seqrite Terminator**> Settings> Dynamic DNS**. The following screen is displayed.



Dynamic DNS

DynaDNS Agent: ● Enabled ○ Disabled

Host Name: . ------ Select Domain ------

Login User ID:

Password:

WAN Interface: EXT-1 : 10.10.104.213

IP Update Interval: 30 Minutes (Max Time 2 Hours)

2. Ensure that the Dynamic DNS is set to **Enabled**.
3. Enter the **Host Name** and select the **Domain**. This is provided by the Dynamic DNS service provider.
4. Enter the **Login User ID** and **Password** of your DDNS account.
5. Select the **WAN Interface**. These are the WAN interface that you have configured in the Interface section. (See **Interface** for more details.)
6. Select the **IP Update Interval** in minutes. Terminator will resync the DNS and check whether there is any change in IP address and updates it after the configured time interval.
7. Click **Save**.

DHCP

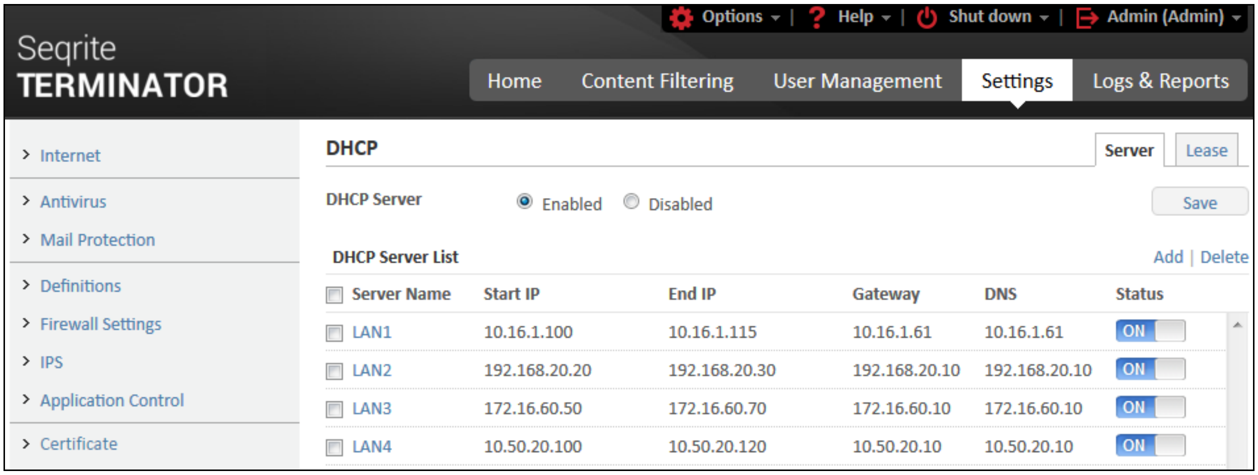
Dynamic Host Configuration Protocol (DHCP) allows you to assign network-parameters automatically to the devices from a DHCP server. The DHCP server feature is useful as it easily allows you to add new machines to the network.

Seqrite Terminator acts as a DHCP server for your network and uses it to assign 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

To add a DHCP server, follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > DHCP**.

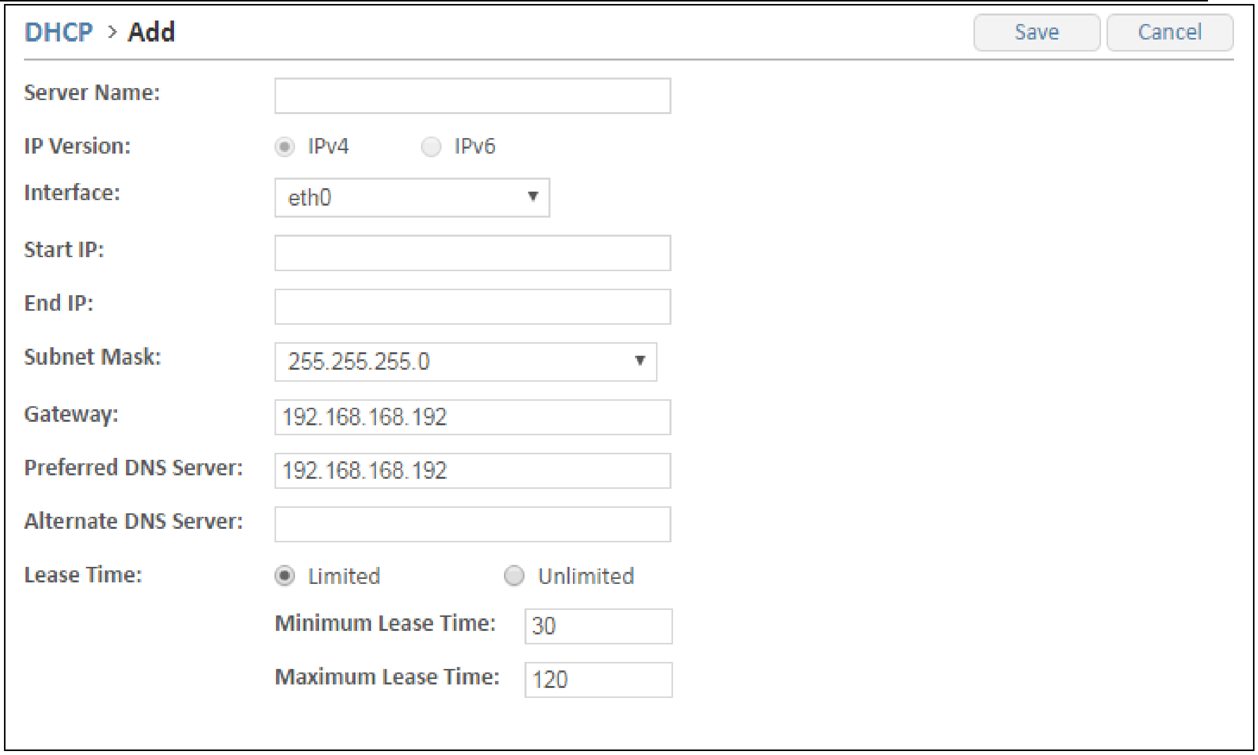


DHCP Server ● Enabled ○ Disabled

DHCP Server List

□ Server Name	Start IP	End IP	Gateway	DNS	Status
□ LAN1	10.16.1.100	10.16.1.115	10.16.1.61	10.16.1.61	ON
□ LAN2	192.168.20.20	192.168.20.30	192.168.20.10	192.168.20.10	ON
□ LAN3	172.16.60.50	172.16.60.70	172.16.60.10	172.16.60.10	ON
□ LAN4	10.50.20.100	10.50.20.120	10.50.20.10	10.50.20.10	ON

2. Select the **Enabled** option.
3. Click **Add**. The DHCP Add screen is displayed.



DHCP > Add

Server Name:

IP Version: ● IPv4 ○ IPv6

Interface: eth0

Start IP:

End IP:

Subnet Mask: 255.255.255.0

Gateway: 192.168.168.192

Preferred DNS Server: 192.168.168.192

Alternate DNS Server:

Lease Time: ● Limited ○ Unlimited

Minimum Lease Time: 30

Maximum Lease Time: 120

The following table describes the fields on page:

Field	Description
Server Name	Name of server you want to set to identify.
IP Version	You can select either IPv4 or IPv6 here. 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.
Interface	The LAN interface on which the DHCP server is running, by default it is set to Eth0.
Start IP	Start of DHCP IP address range, this IP address should be in the same network to which Eth0 is configured.
End IP	End of DHCP IP address range, this IP address should be in the same network as the Eth0 and the IP address of Eth0 of Terminator should not come in between the range.
Subnet Mask	Subnet Mask which should be set for the clients.
Gateway	Set the gateway which will be set as a default gateway to clients, by default it is the IP address of Eth0 of Terminator.

Field	Description
Preferred DNS Server	DNS which will be set as Preferred DNS to clients.
Alternate DNS Server	DNS which will be set as Secondary DNS to clients.
Lease Time	You can select it to be Limited or Unlimited. If you select Limited, then the following options are displayed: Minimum Lease time: The lease time after which the client will request to renew the lease. Maximum Lease time: The lease time after which DHCP server will free the IP address if no response is returned from the client.

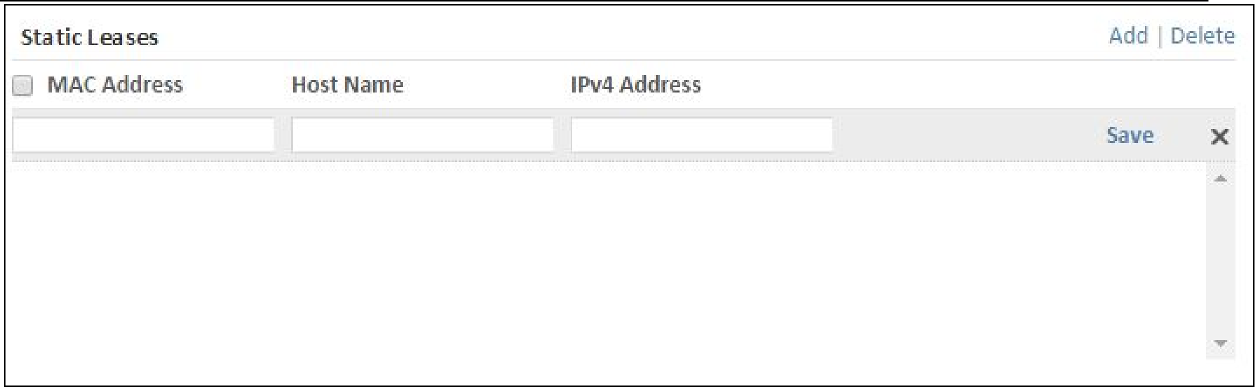
4. Click **Save.**

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.

To add a static Lease follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > DHCP**.
2. Click **Add** in the **Static Leases** section.



3. Enter the following details:
   1. **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.
   2. **Hostname**: Set the hostname of client.
   3. **IPv4 Address**: Set the IPv4 address to bind. The IP address will be assigned to the user's computer.
4. Click **Save**.

Deleting DHCP servers

To delete a DHCP server follow the steps given below:

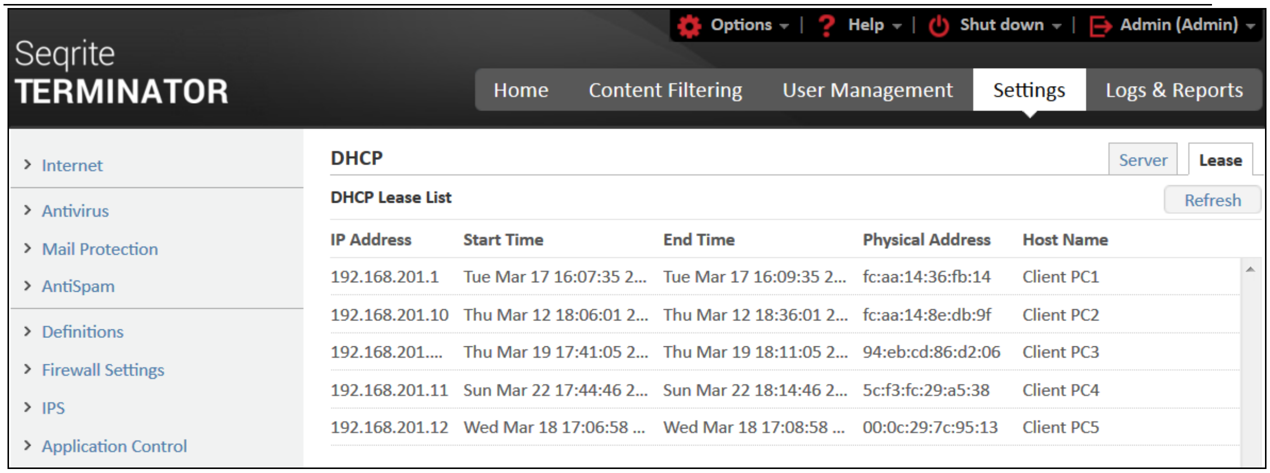
1. Log on to Seqrite Terminator **> Settings> DHCP**. The DHCP server list is displayed that has the Server Name, Start IP address, End IP Address, Gateway IP address, DNS and a Status button.
2. Select the required DHCP Server and click **Delete.**

Viewing 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.

To view DHCP lease details, follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > DHCP**.
2. Click **Lease**. The Lease list is displayed containing the IP Address, Lease Start Time, End Time Physical Address and Host Name.



DHCP Lease List

IP Address	Start Time	End Time	Physical Address	Host Name
192.168.201.1	Tue Mar 17 16:07:35 2...	Tue Mar 17 16:09:35 2...	fc:aa:14:36:fb:14	Client PC1
192.168.201.10	Thu Mar 12 18:06:01 2...	Thu Mar 12 18:36:01 2...	fc:aa:14:8e:db:9f	Client PC2
192.168.201....	Thu Mar 19 17:41:05 2...	Thu Mar 19 18:11:05 2...	94:eb:cd:86:d2:06	Client PC3
192.168.201.11	Sun Mar 22 17:44:46 2...	Sun Mar 22 18:14:46 2...	5c:f3:fc:29:a5:38	Client PC4
192.168.201.12	Wed Mar 18 17:06:58 ...	Wed Mar 18 17:08:58 ...	00:0c:29:7c:95:13	Client PC5

3. To refresh the list click **Refresh.**

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 or the route information that is calculated using dynamic routing algorithms.

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

- Static Routing
- Policy Based Routing (PBR)

Static Routing

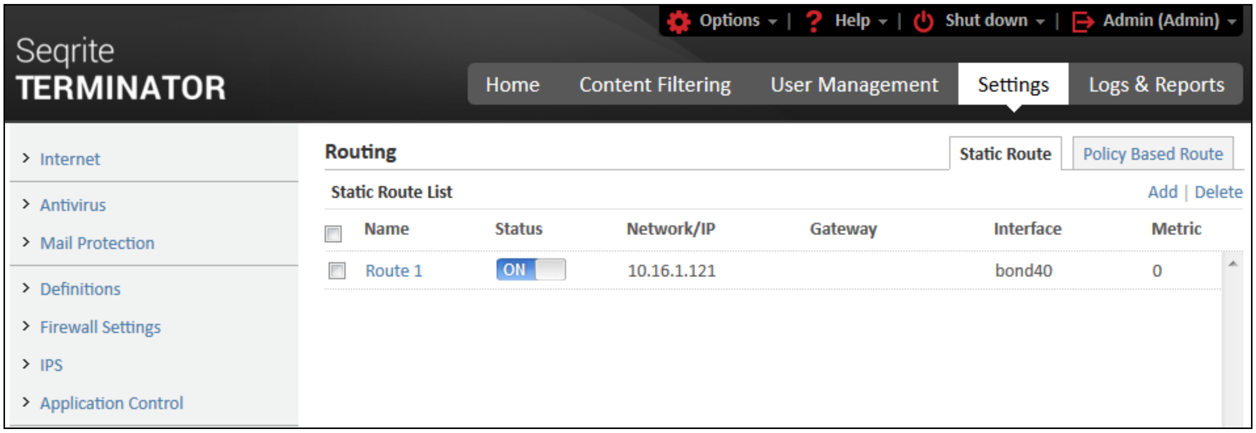
Static routing helps to define explicit paths between two routers and is not updated automatically. You must manually reconfigure the static route whenever network changes occur.

The Static Route feature in Terminator allows you to configure a route using which the Terminator 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. Using the Terminator you can add or delete the routes. If you set the route to OFF, then that static route is currently removed from the device’s routing tables.

Adding a Static Route

To add a Static route, follow the steps given below:

1. Log on to Seqrite Terminator**> Settings> Routing**. The Static Routing page is displayed which displays the list of added routes.

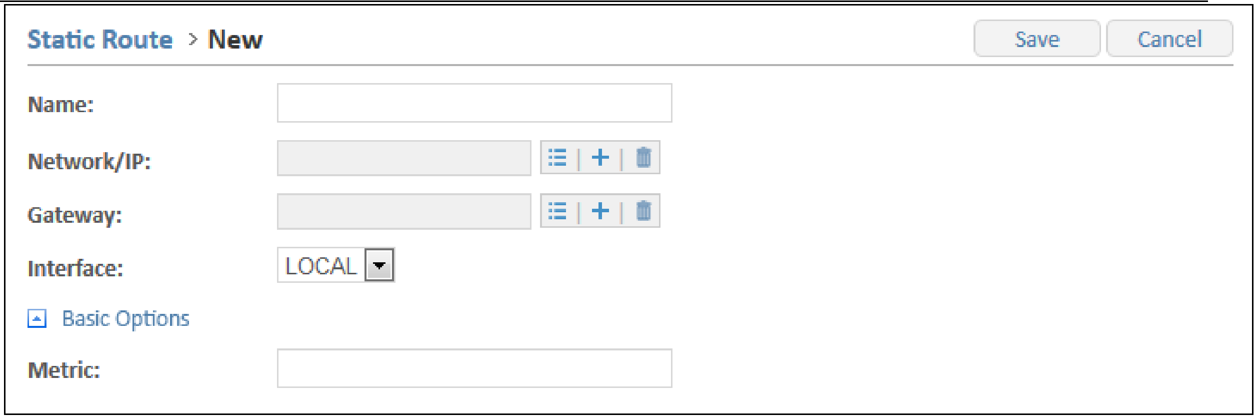


Routing

Static Route List

□	Name	Status	Network/IP	Gateway	Interface	Metric
□	Route 1	ON	10.16.1.121		bond40	0

2. Click **Add** to add a route. On clicking **Add**, the following page is displayed.



Name:

Network/IP:

Gateway:

Interface: LOCAL

Basic Options

Metric:

3. Enter the **Name** of the new route.
4. Configure the destination / target IP using the **Network IP** field**.** You can browse, add, or delete, the Network definitions using the designated icons.
5. Configure the next hop in the route using the **Gateway** field. You can browse, add, or delete the Network definitions using the designated icons.
6. Select the **Interface** for the routing table through which you want the packets to be transmitted.
7. You can use the **Advanced Options** to configure the **Metric** option. 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.
8. Click **Save**.

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 in Terminator 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

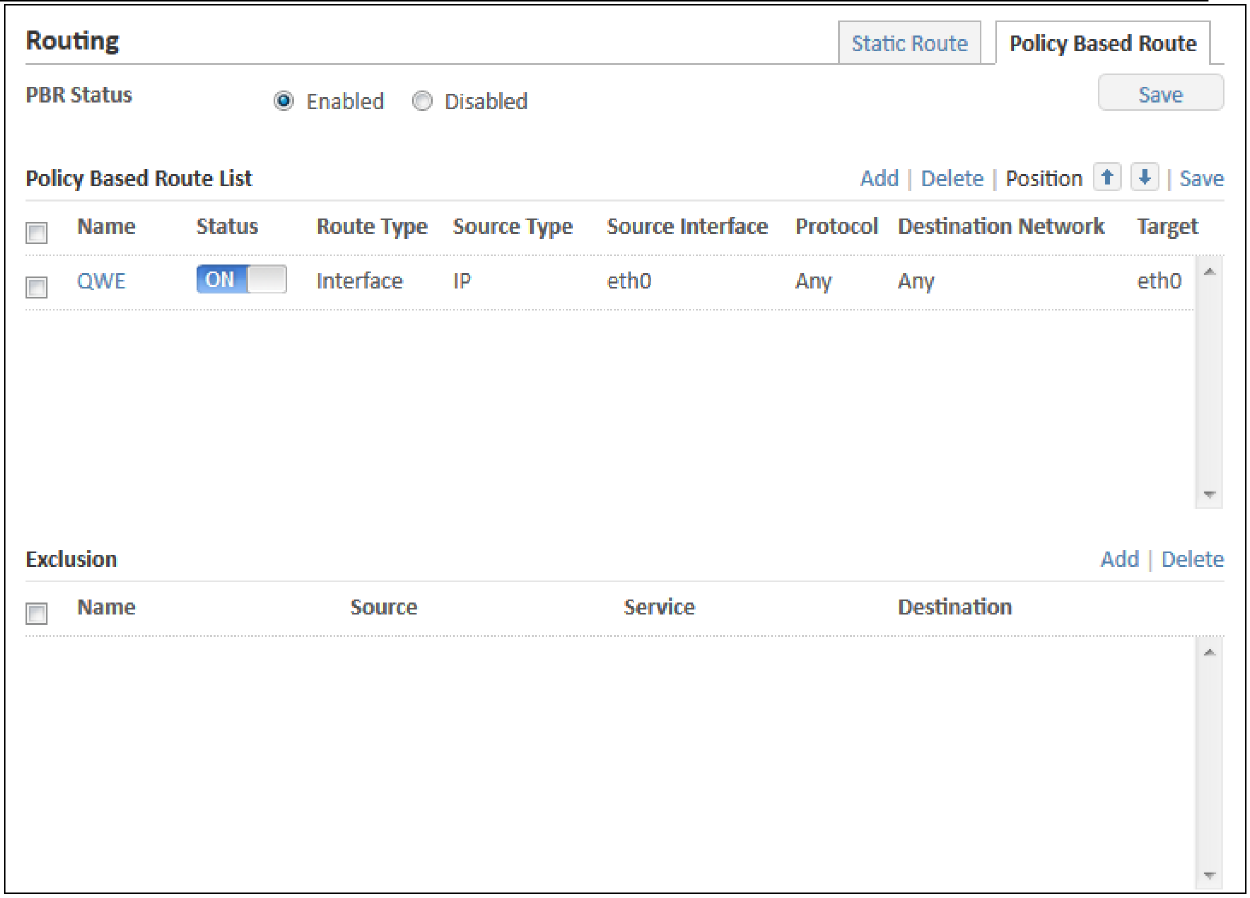
If network traffic passing through Seqrite Terminator satisfies the provided criteria, traffic will be forwarded through a target network interface link or target gateway.

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

To enable policy based routing, follow the steps given below:

1. Log on to the **Seqrite Terminator> Settings > Routing> Policy Based Route**.



PBR Status ● Enabled ○ Disabled

Policy Based Route List

□	Name	Status	Route Type	Source Type	Source Interface	Protocol	Destination Network	Target
□	QWE	ON	Interface	IP	eth0	Any	Any	eth0

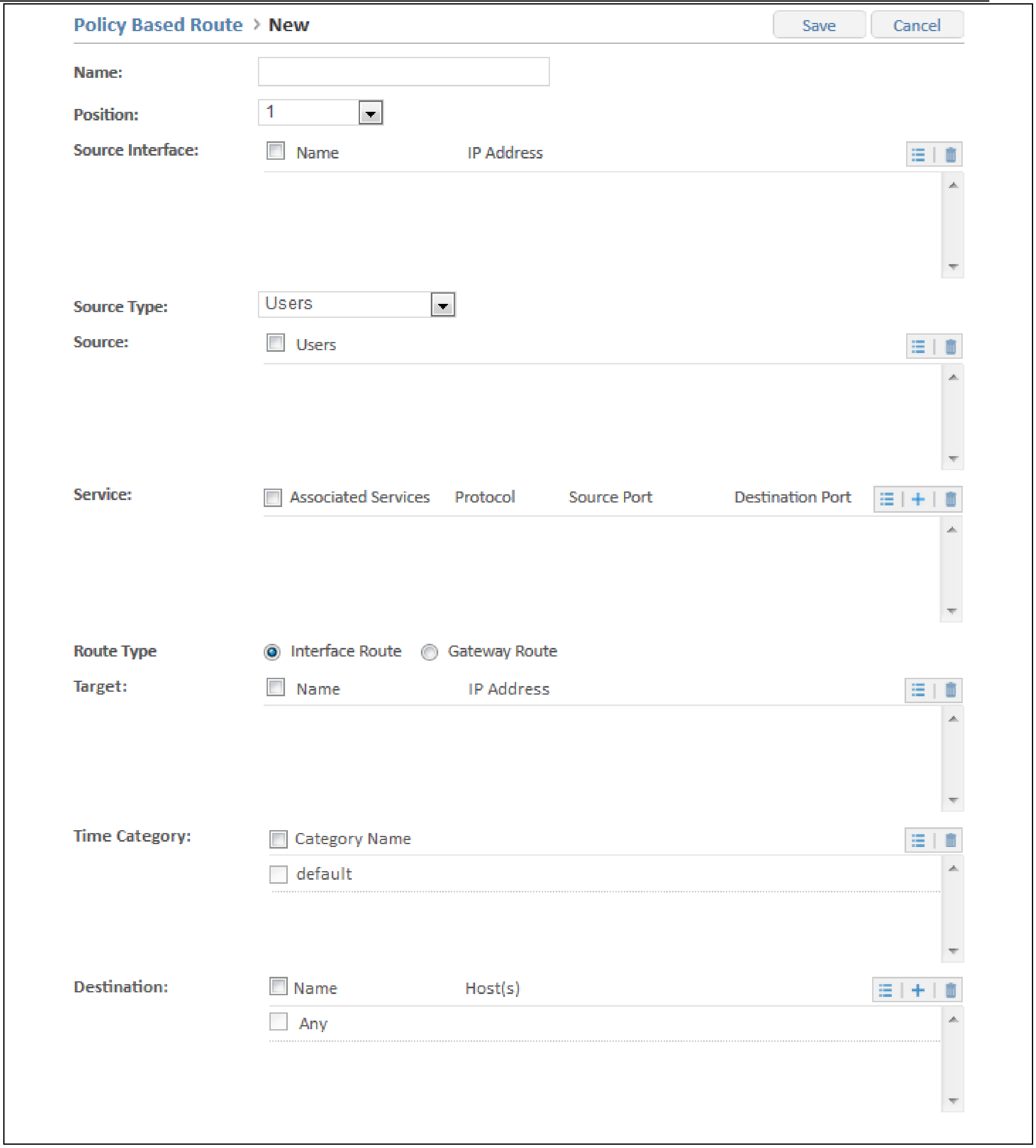
□	Name	Source	Service	Destination

2. Select **Enabled** for the PBR status.
3. Click **Save**.

Adding routing policies

To add a routing policy follow the steps given below:

1. Log on to the **Seqrite Terminator > Settings > Routing> Policy Based Route**.
2. Click **Add**. The following page is displayed.



Policy Based Route › New

Name:

Position: 1

Source Interface: □ Name IP Address

Source Type: Users

Source: □ Users

Service: □ Associated Services Protocol Source Port Destination Port

Route Type ● Interface Route ○ Gateway Route

Target: □ Name IP Address

Time Category: □ Category Name

□ default

Destination: □ Name Host(s)

□ Any

The following table describes the fields on the page:

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

Field	Description
	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 interface. 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 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 are displayed. (See **Definitions** for more details of Network Definition)

3. Click **Save**.

Deleting a routing policy

To delete a routing policy follow the steps given below:

1. Log on to the Seqrite Terminator **Settings** > **Routing**.
2. Select the policy that you want to delete, click **Delete.**
3. Click **OK** on the confirmation box. The policy is deleted.

Changing the priority of policies

To change priority of the policies follow the steps given below:

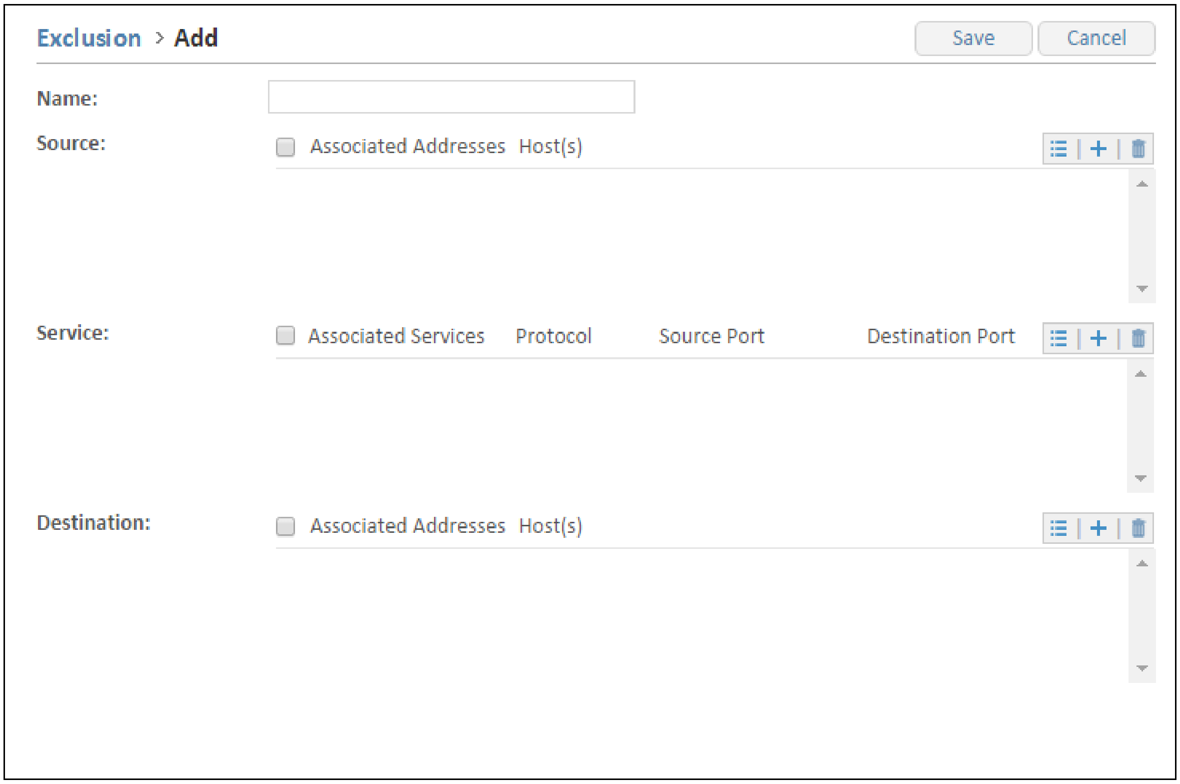
1. Log on to the Terminator> **Settings** > **Routing**.
2. Select the policy for which you want to change the priority, click the **Change Priority** arrows, up or down as required to change the priority.
3. Click **Save**.

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 criteria in Policy Based Route Exclusion for this network traffic.

To exclude interface from PBR follow the steps given below:

1. Log on to the **Seqrite Terminator**> **Settings > Routing**> **Policy Based Route**.
2. Click **Add** link under the **Exclusion** section.



Exclusion > Add

Name:	
Source:	□ Associated Addresses Host(s)
Service:	□ Associated Services Protocol Source Port Destination Port
Destination:	□ Associated Addresses Host(s)

3. 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**.
7. Click **Save**.

Load Balance and Failover

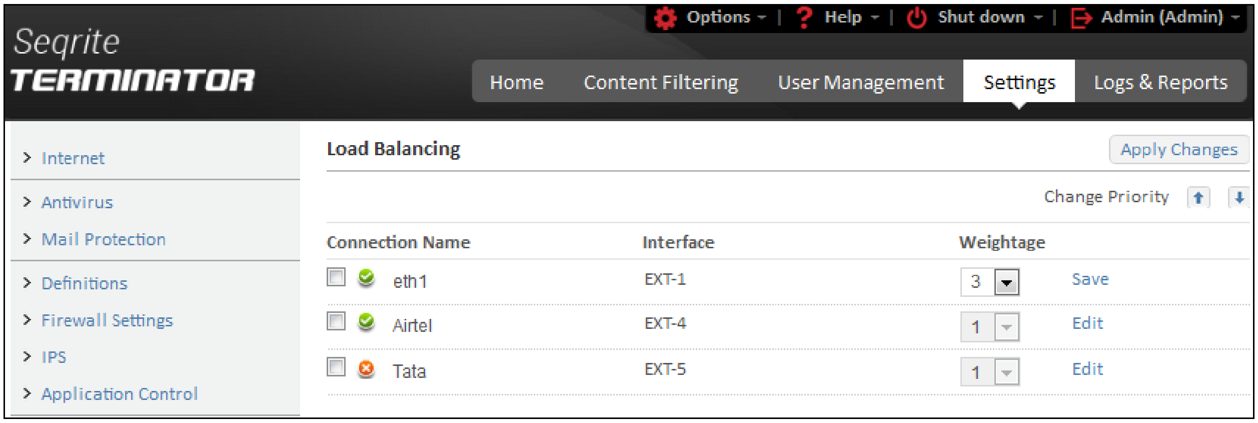
Load balancing helps in balancing the Internet traffic in case you have more than one Internet connections. You can set the weightage for the Internet connections which helps to describe the amount of traffic that will pass through the respective WAN interface. Higher the weightage more traffic is allowed 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.

Terminator 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 is set as default interface.

To configure load balancing, follow the steps given below:

1. Log on to Seqrite Terminator**> Settings> Load Balancing**. The Load Balancing screen is displayed with the list of the configured interfaces connected to the Internet.



Load Balancing

Connection Name	Interface	Weightage	
□ ✓ eth1	EXT-1	3	Save
□ ✓ Airtel	EXT-4	1	Edit
□ ✗ Tata	EXT-5	1	Edit

2. Select an interface and click **Edit**.
3. Select the **Weightage** value for each interface.

   Note: In case no setting for weightage is configured, the load is split equally among connections.
4. Click **Save**.

   Note: You can change the priority as required using the **Change Priority** button.

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 Terminator to filter the information coming in and going out of your private network. The Seqrite Terminator 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 Terminator 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.

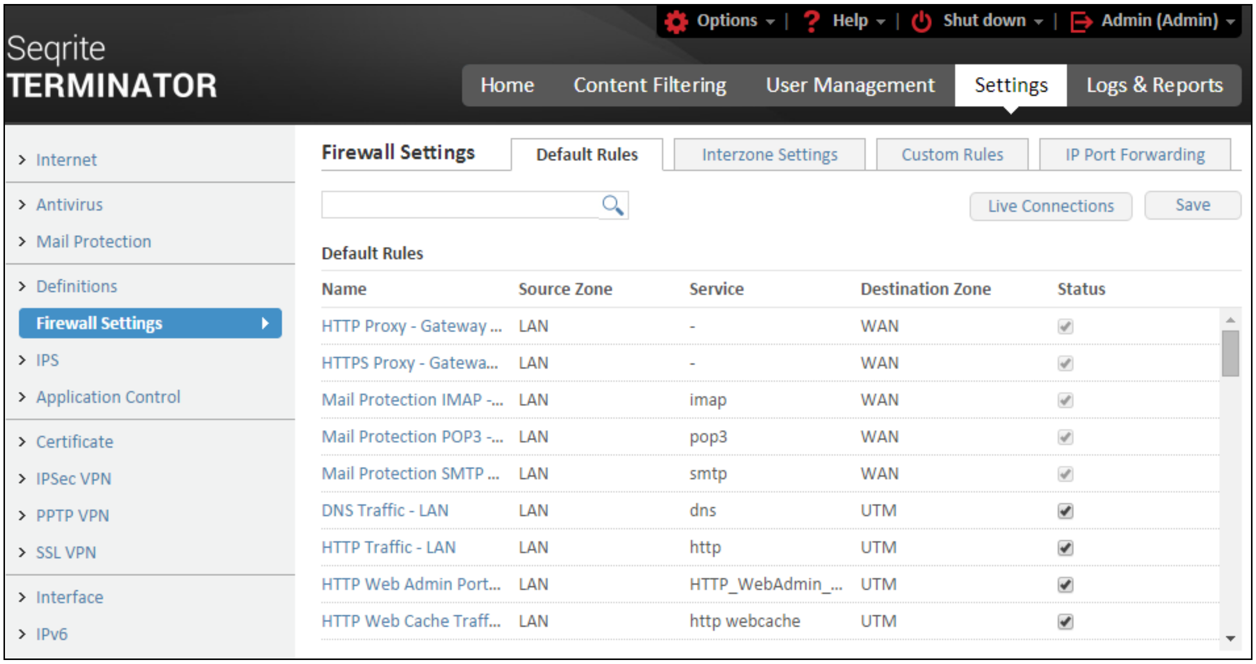
Default Firewall rules

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

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

To view the default firewall rules follow these steps:

1. Log on to Seqrite Terminator **> Settings > Firewall Settings.** The following page is displayed.



Default Rules

Name	Source Zone	Service	Destination Zone	Status
HTTP Proxy - Gateway ...	LAN	-	WAN	☑
HTTPS Proxy - Gatewa...	LAN	-	WAN	☑
Mail Protection IMAP -...	LAN	imap	WAN	☑
Mail Protection POP3 -...	LAN	pop3	WAN	☑
Mail Protection SMTP ...	LAN	smtp	WAN	☑
DNS Traffic - LAN	LAN	dns	UTM	☑
HTTP Traffic - LAN	LAN	http	UTM	☑
HTTP Web Admin Port...	LAN	HTTP_WebAdmin_...	UTM	☑
HTTP Web Cache Traff...	LAN	http webcache	UTM	☑

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

3. You can enable / disable the default rule using the checkbox in the **Status** column of the table.

4. You can search the Default rules by name using the search textbox.

5. Click on **Live Connection** to view the list of established connections through Terminator.

6. You can apply filters on connections by protocol or destination port or both. You can also search connections with source/destination IP address.

7. You can select to drop the established connections. Click the **Cancel** button to cancel the service configuration.

Inter-zone Settings

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 service 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.

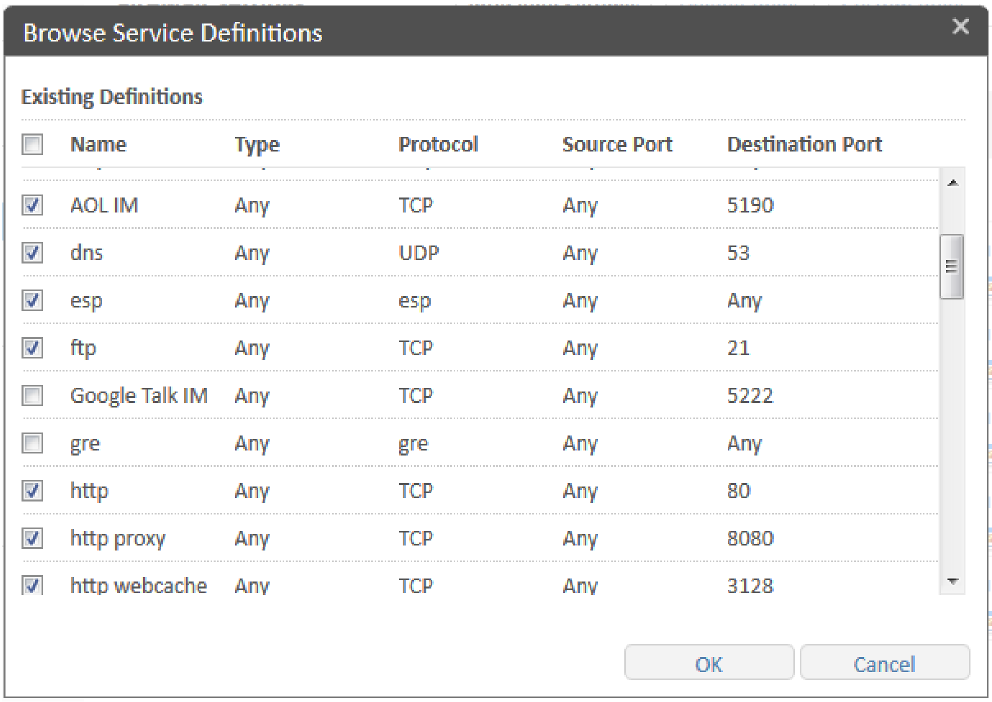
The one click global configuration on the Inter-zone settings page allows you to configure well known services easily.

To configure global firewall rules follow these steps:

1. Log on to Seqrite Terminator **> Settings > Firewall > Interzone Settings**. The following page is displayed

   <Image>

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



Browse Service Definitions

Existing Definitions

□	Name	Type	Protocol	Source Port	Destination Port
☑	AOL IM	Any	TCP	Any	5190
☑	dns	Any	UDP	Any	53
☑	esp	Any	esp	Any	Any
☑	ftp	Any	TCP	Any	21
□	Google Talk IM	Any	TCP	Any	5222
□	gre	Any	gre	Any	Any
☑	http	Any	TCP	Any	80
☑	http proxy	Any	TCP	Any	8080
☑	http webcache	Any	TCP	Any	3128

3. Select the Service Definition that you want to allow for the source-destination zone pair. Click **OK**.

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

5. You can also apply NAT to LAN - WAN and DMZ- WAN source- destination pairs, to translate source IP address of outgoing packets. 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.

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.

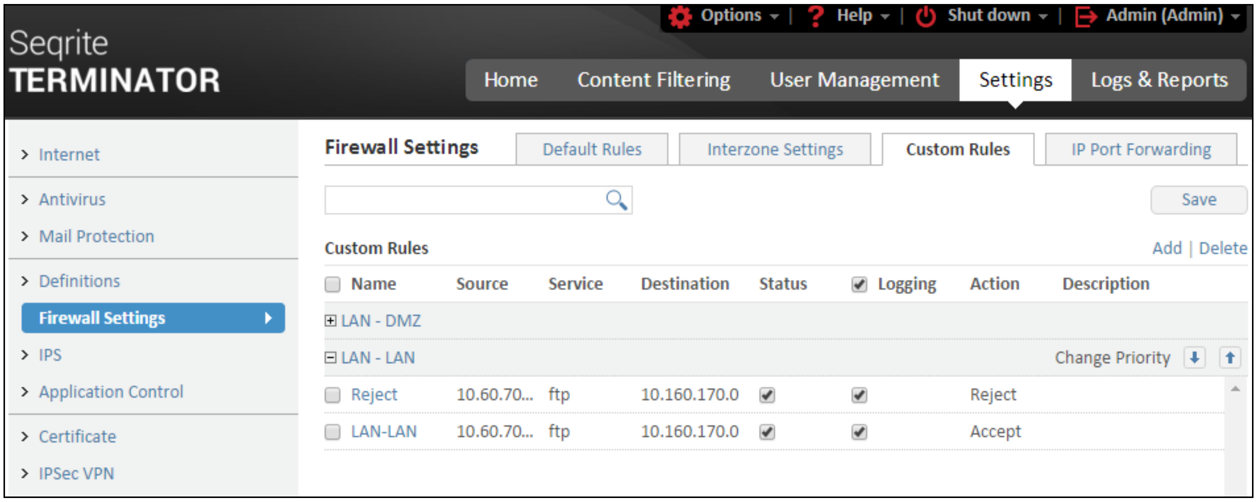
Note:

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

To view custom firewall rules:

1. Log on to Seqrite Terminator **> Settings > Firewall Settings> Custom Rules**. The following page is displayed.



□ Name	Source	Service	Destination	Status	☑ Logging	Action	Description
⊞ LAN - DMZ							
⊟ LAN - LAN							
□ Reject	10.60.70...	ftp	10.160.170.0	☑	☑	Reject	
□ LAN-LAN	10.60.70...	ftp	10.160.170.0	☑	☑	Accept	

2. The Custom Firewall page displays the group wise list of firewall rules.

3. Click on the Group name to view firewall rules under the particular group.

4. Set the status of the Rule as enabled/ disabled using the button provided under the **Status** column.

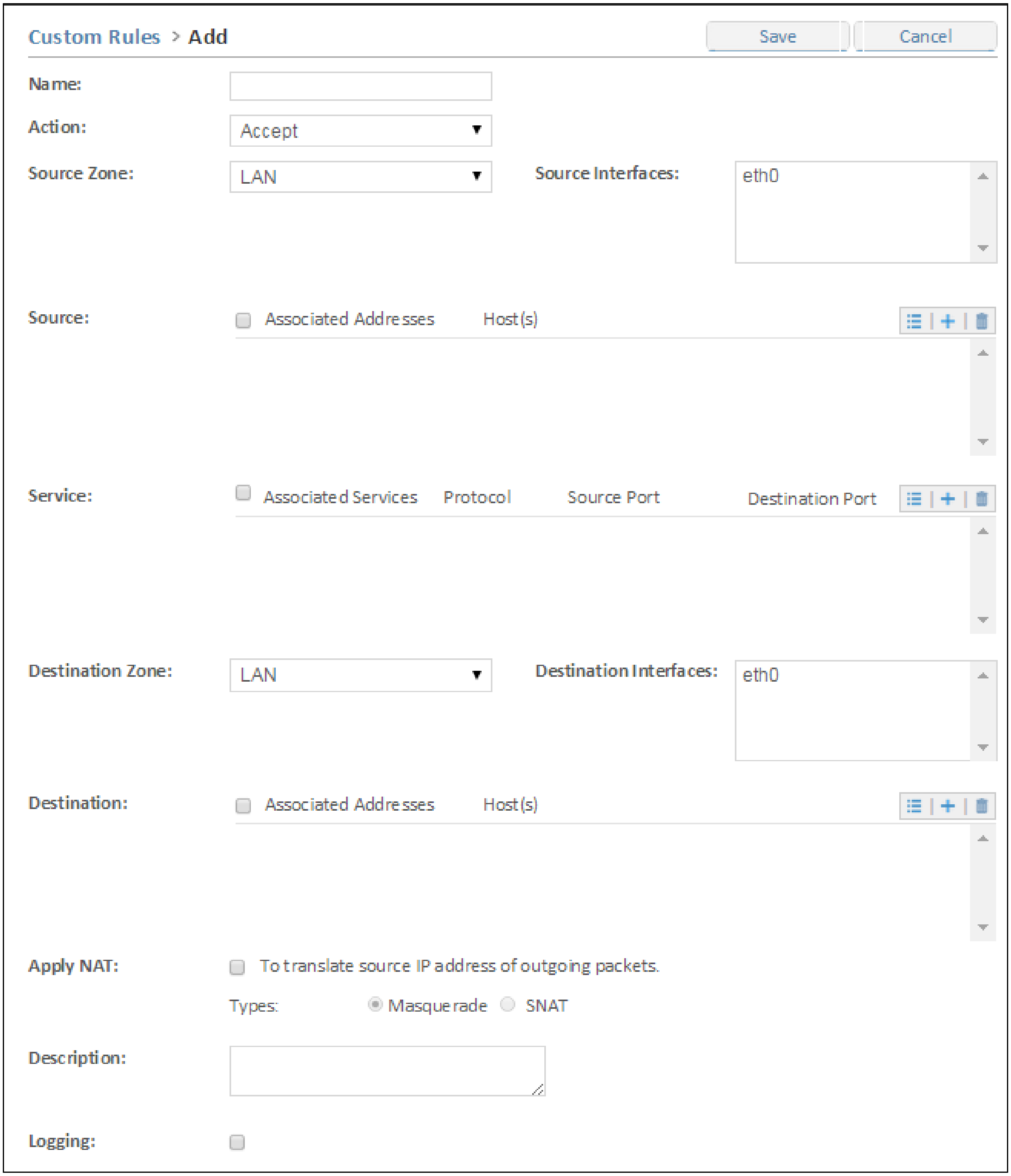
5. Select the logging option under the **Logging** column to enable logging for the firewall rules.

6. Click **Save**.

Adding Firewall Rules

To create a firewall rule, follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > Firewall Settings> Custom Rules**. The following page is displayed.
2. Click **Add**. The Add Firewall settings page will be displayed.



Custom Rules > Add

Name:

Action: Accept

Source Zone: LAN

Source Interfaces: eth0

Source: □ Associated Addresses Host(s)

Service: □ Associated Services Protocol Source Port Destination Port

Destination Zone: LAN

Destination Interfaces: eth0

Destination: □ Associated Addresses Host(s)

Apply NAT: □ To translate source IP address of outgoing packets.

Types: ● Masquerade ○ SNAT

Description:

Logging: □

3. The following table explains the fields on the page.

Field	Description
Name	Enter a **Name** for the rule.

Field	Description
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.
Source Zone	Select appropriate source zone from the Source Zone list. Source zone list contains LAN, WAN, DMZ, VPN, UTM and, Bridge.
Source interface	Enter the Source Interface.
Source	Select the source host or network address to which the rule will be applied. You can browse, 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 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.
Destination	Select the destination host or network address to which the rule will be applied. You can browse, add or delete the Network Definition using the respective icons.
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

Field	Description
	option requires IP address of outgoing interface to be entered.
Description	Enter the description for the firewall rule.
Logging	Select this option if you want to log activities for the firewall rule.

4. Click **Save**.

Deleting a Firewall rule

To delete a firewall rule, follow the steps given below:

1. Log on to Seqrite Terminator> **Settings > Firewall Settings> Custom Rules**. The following page is displayed with the list of rules:
2. Select the firewall rule that you want to delete and click **Delete**.

IP Port Forwarding

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.

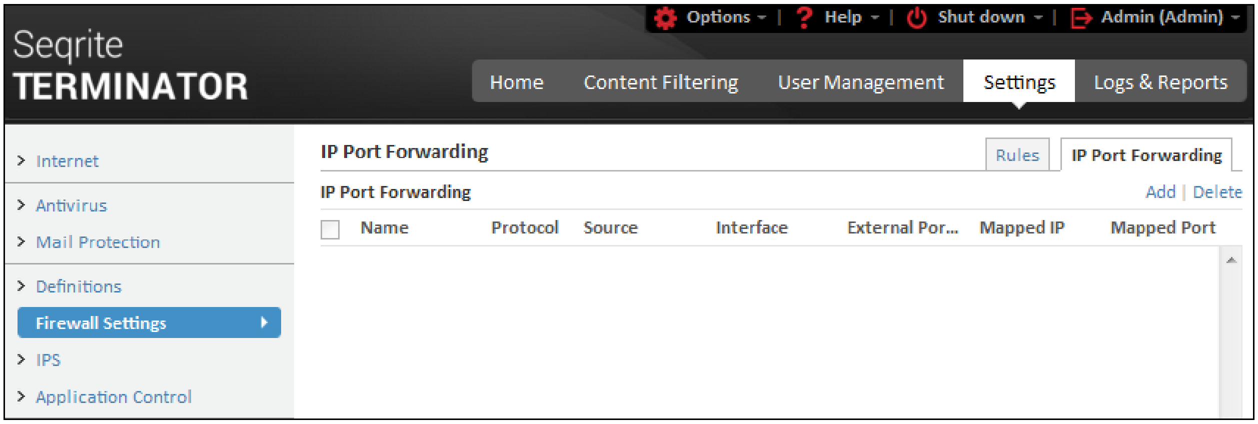
Using the IP/Port forwarding feature in Terminator you can make a host on your network accessible to host on the Internet (outside your network), even though they are behind the Terminator. Entire IP address can be forwarded to allow access to all the ports of a computer or only specific ports can be 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

To view list of IP port forwarding rules follow these steps:

1. Log on to Seqrite Terminator **> Settings > Firewall > IP Port Forwarding**. Following screen is displayed

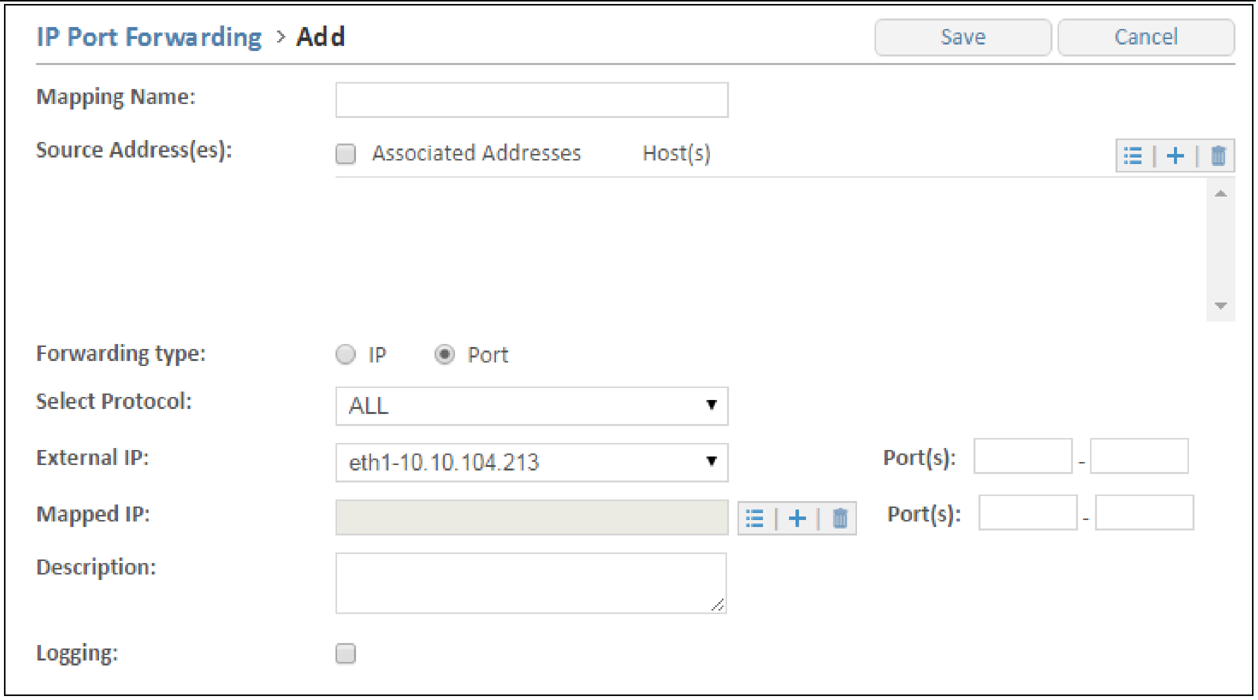


2. This page displays the list of IP port forwarding rules.
3. Set the status of the Rule as enabled/ disabled using the button provided under the **Status** column.
4. Select the logging option under the **Logging** column to enable logging for the rules.
5. Click **Save**.

Adding IP port forwarding rule

To add IP Port Forwarding rule, follow these steps:

1. Log on to Seqrite Terminator **> Settings > Firewall > IP Port Forwarding**. Following screen is displayed.
2. Click **Add**. The following screen is displayed.



Mapping Name:

Source Address(es): □ Associated Addresses Host(s)

Forwarding type: ○ IP ● Port

Select Protocol: ALL

External IP: eth1-10.10.104.213 Port(s): -

Mapped IP: Port(s): -

Description:

Logging: □

3. Enter the **Mapping Name**.
4. Browse or add **Source Address(es).**
5. 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).
6. Select a protocol from the **Select Protocol** list. Protocol list has options as ALL, TCP and UDP.
7. Select **External IP.** External IP is the WAN interface IP address which will be used in forwarding. Public computers access this IP address**.**
8. 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.
9. Enter the **Description** for the rule.
10. Select the **Logging** option, if you want to log the activities related to the rule.
11. Click **Save**.

Deleting IP port forwarding rule

To delete a firewall rule, follow the steps given below:

1. Log on to Seqrite Terminator> **Settings > Firewall Settings> IP port forwarding**. The following page is displayed with the list of rules:
2. Select the rule that you want to delete and click **Delete**.

VPN

Virtual private network (VPN) is a network that is constructed to connect two private network, 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 Terminator 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 Terminator 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.

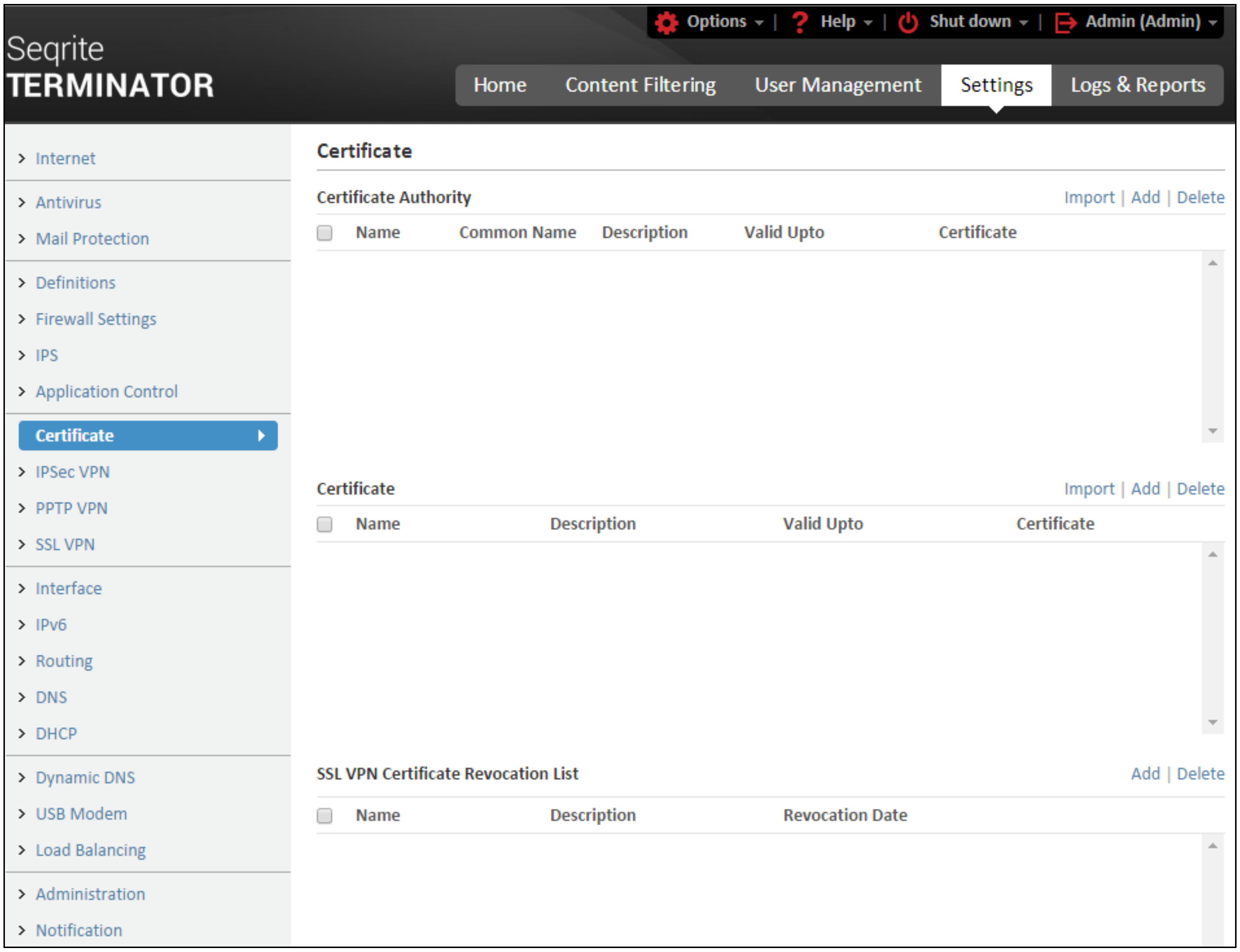
Certificates

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 Terminator 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 Terminator helps you to maintain a revocation list of certificates.

To manage certificates:

1. Log on to Seqrite Terminator **> Settings > Certificates.** The following page is displayed.



Certificate

Certificate Authority

□	Name	Common Name	Description	Valid Upto	Certificate

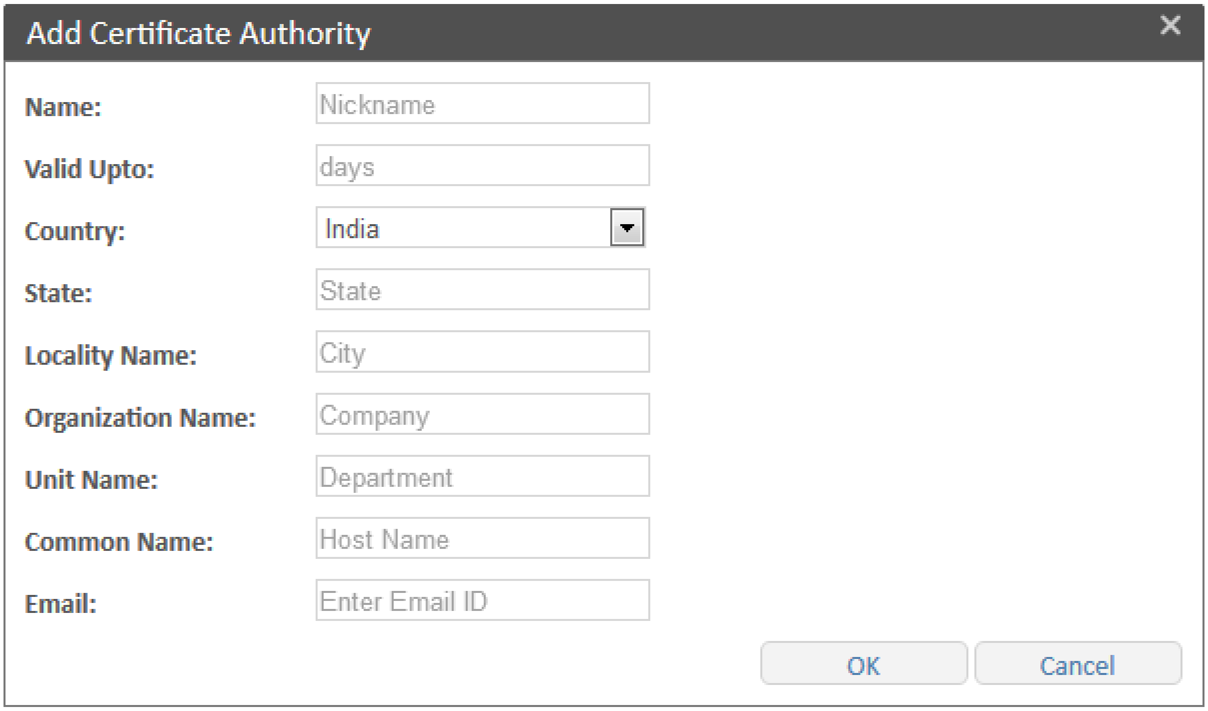
Certificate

□	Name	Description	Valid Upto	Certificate

SSL VPN Certificate Revocation List

□	Name	Description	Revocation Date

2. The page is divided in the following three sections:
   - Certificate Authority
   - Certificates
   - SSL VPN Revocation list
3. To add Certificate Authority / certificates, click **Add** in the respective section. The **Add Certificate Authority / Add Certificate** popup is displayed.



Add Certificate Authority

Name: Nickname

Valid Upto: days

Country: India

State: State

Locality Name: City

Organization Name: Company

Unit Name: Department

Common Name: Host Name

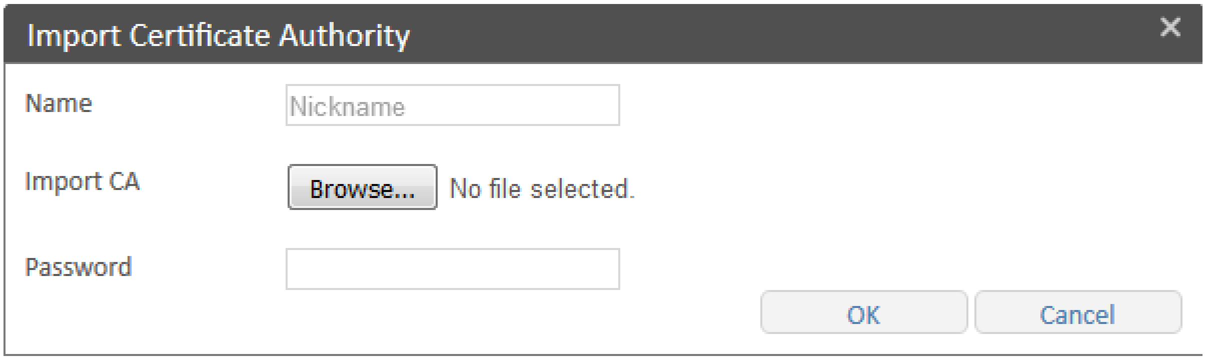
Email: Enter Email ID

4. Enter the details such as Name, Valid Upto, Country, State, Locality name, Organization Name, Unit Name, Common Name, and Email and click **OK**.

   Note:

   - While adding Certificate, you need to select the associated CA.
   - Space is not allowed in Name and Common Name.

5. You can import third party certificates and Certificate Authorities. To import certificate / Certificate Authority click **Import** in the respective section, enter a Name, choose a file, enter the password and click **Ok**.



Import Certificate Authority

Name: Nickname

Import CA: No file selected.

Password:

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.

6. The **SSL VPN Revocation List** displays the list of blacklisted connections, description and the date they were added to the revocation list. This can be done to stop connection 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 and click **Save**.

IPsec

Seqrite Terminator 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. It 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.

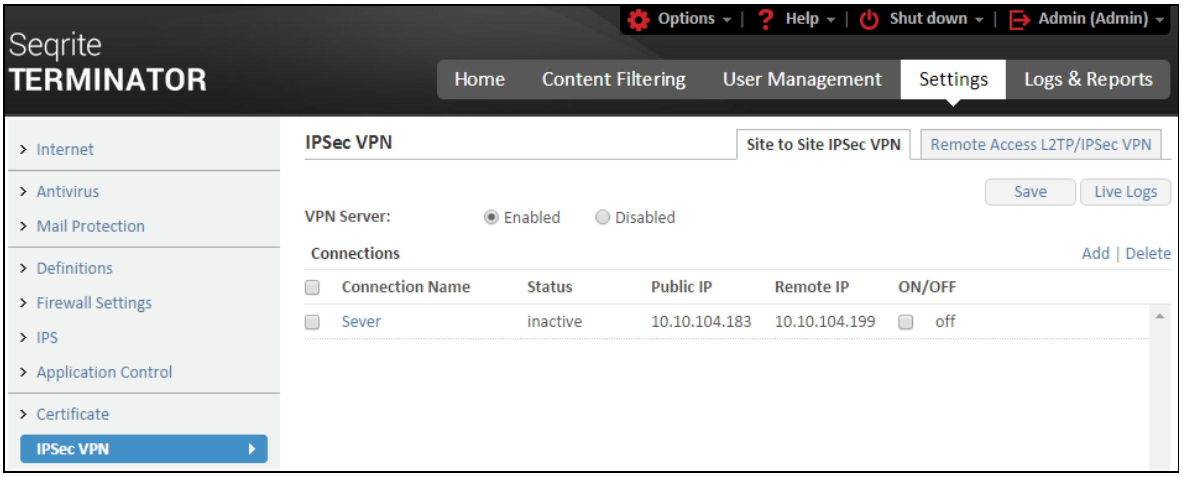
You can also view the Live logs of IPSec VPN connections, by clicking the Live logs button. These logs indicate the current status of IPSecVPN service.

Adding Site to Site IPSec VPN

Using the Site to Site IPSec VPN connection various branch networks can access the remote network.

To Add an IPSec VPN server, follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > IPSec VPN**. The IPSec VPN screen is displayed wit the list of VPN connection. You can also add or delete IPSec VPN.



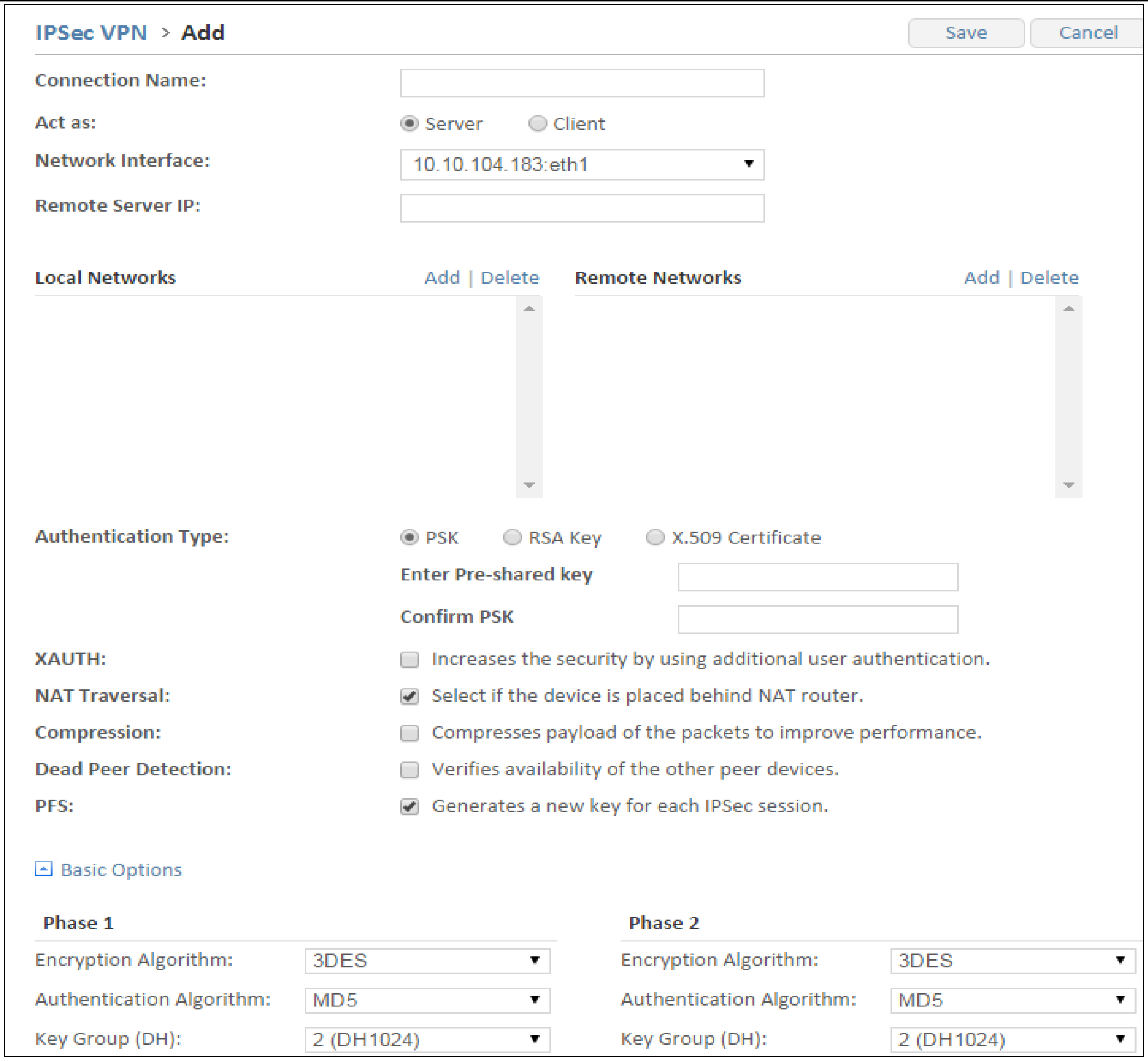
IPSec VPN

VPN Server: ● Enabled ○ Disabled

Connections

□	Connection Name	Status	Public IP	Remote IP	ON/OFF
□	Sever	inactive	10.10.104.183	10.10.104.199	□ off

2. Select the VPN Server as **Enabled.**
3. To Add Site to Site IPSecC VPN click **Add**. The IPSec VPN Add screen is displayed.



IPSec VPN > Add

Connection Name:

Act as: ● Server ○ Client

Network Interface: 10.10.104.183:eth1

Remote Server IP:

Authentication Type: ● PSK ○ RSA Key ○ X.509 Certificate

Enter Pre-shared key

Confirm PSK

XAUTH: ☐ Increases the security by using additional user authentication.

NAT Traversal: ☑ Select if the device is placed behind NAT router.

Compression: ☐ Compresses payload of the packets to improve performance.

Dead Peer Detection: ☐ Verifies availability of the other peer devices.

PFS: ☑ Generates a new key for each IPSec session.

Phase 1		Phase 2	
Encryption Algorithm:	3DES	Encryption Algorithm:	3DES
Authentication Algorithm:	MD5	Authentication Algorithm:	MD5
Key Group (DH):	2 (DH1024)	Key Group (DH):	2 (DH1024)

The following table explains the fields on page:

Field Name	Description
Connection Name	Enter the Connection Name. This is the unique name for the connection used for identification
Act As	Set the server to act as. • Server: On selecting this option your server will act as the main server. • Client: On selecting this option your server will act as Client server.
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.
Remote Server IP	Enter the Remote Server IP: This is the remote public IP on which the VPN server is running.
Local Networks.	Select / Enter the Local Networks. You can select multiple Local networks.
Remote Network address	Select / Enter the Remote Network address. This are the Network address of the Remote private network.
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.
XAuth	Along with the above authorization type, you can also add extra authentication using the XAuth option. If you select this option and acting as a server, then you need to set a username and password for authentication and share this with the Client. Note: Incase 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, 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.

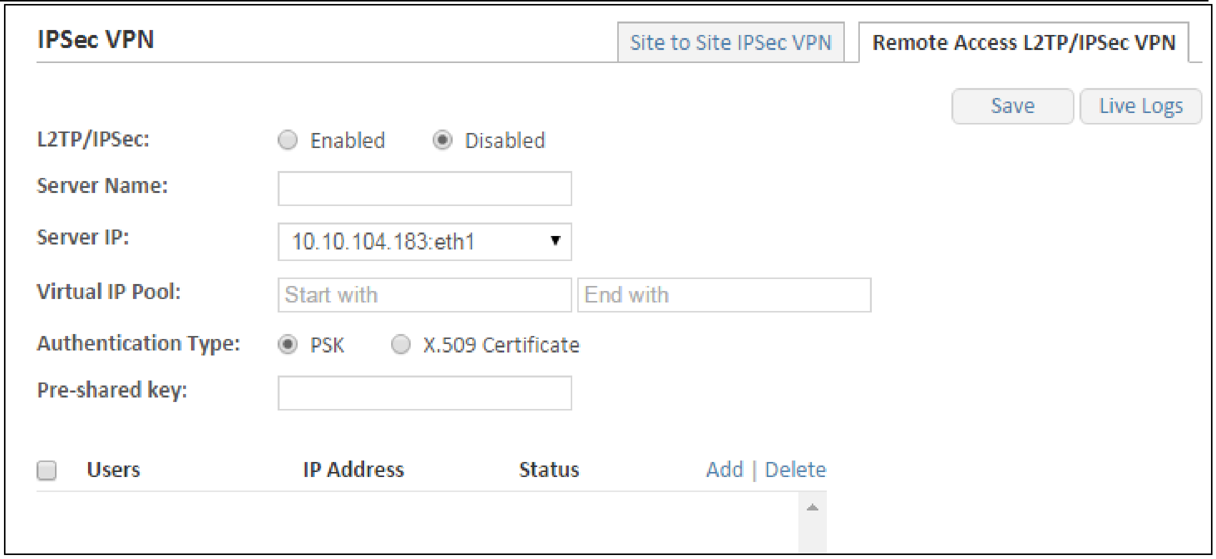
4. Click **Save** after entering all the required details.

Adding a Remote Access L2TP / IPSec VPN

Remote Access L2TP IPSec VPN allows a single PC/Laptop to access the remote network. You can set the Pre Shared Key and X.509 certificates for Authentication and safe access. You can set a pre shared key an add users who can connect to the VPNs.

To add a Remote Access L2TP / IPSec VPV access, follow the steps given below:

1. Log on to Seqrite Terminator**> Settings > IPSec VPN > Remote Access L2TP / IPSec VPN.** The following screen is displayed.


IPSec VPN

L2TP/IPSec: ○ Enabled ● Disabled

Server Name:

Server IP: 10.10.104.183:eth1

Virtual IP Pool: Start with End with

Authentication Type: ● PSK ○ X.509 Certificate

Pre-shared key:

□ Users	IP Address	Status	Add | Delete

2. Select the L2TP/IPSec option as **Enabled**.

3. Enter the **Server name**.

4. Enter the **Server IP**.

5. Enter the **Virtual IP Pool**. These are the IP addresses that will be assigned to the Remote users for accessing the private network.
6. 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.
7. Add the users whom you want to allow access of the remote network. Click **Add** in the **Users** section of the page. Enter the **Username**, **password** and **confirm password**, which will be used by the users to connect to the VPN.
8. Click **Save**.

PPTP VPN

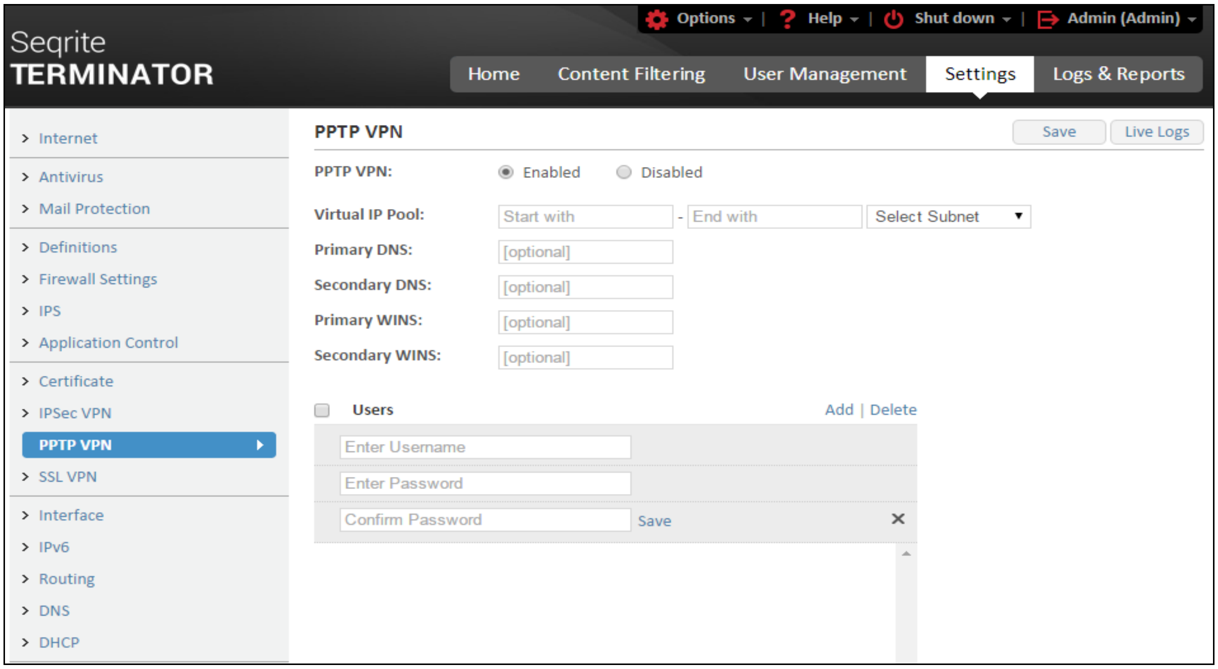
The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks for Single PC access. In Seqrite Terminator, the PPTP VPN allows you to connect single PC to the private network. PPTP uses plain text authentication and MPPE encryption for creating a secure tunnel for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

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

To add a new PPTP VPN connection, follow the steps given below:

1. Log on to Seqrite Terminator**> Settings > PPTP VPN**.
2. Click **Add**. The PPTP Remote Network Access New connection screen is displayed as shown in the figure.



PPTP VPN

PPTP VPN: ● Enabled ○ Disabled

Virtual IP Pool: Start with - End with Select Subnet ▾

Primary DNS: [optional]

Secondary DNS: [optional]

Primary WINS: [optional]

Secondary WINS: [optional]

□ Users Add | Delete

Enter Username

Enter Password

Confirm Password Save ✕

3. Enter the **Connection Name.**
4. Enter **Virtual IP pool**. These are the IP addresses that will be assigned to the Remote users for accessing the private network.
5. Enter the IP address of the Primary / secondary DNS server.
6. Enter the IP address of the primary / secondary WINS server.
7. To Add users who can access the PPTP VPN, click Add in the Users section. Enter the **Username**, **Password and Confirm password** required for user authentication of the user.
8. Click **Save**.

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 roadwarrior 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.

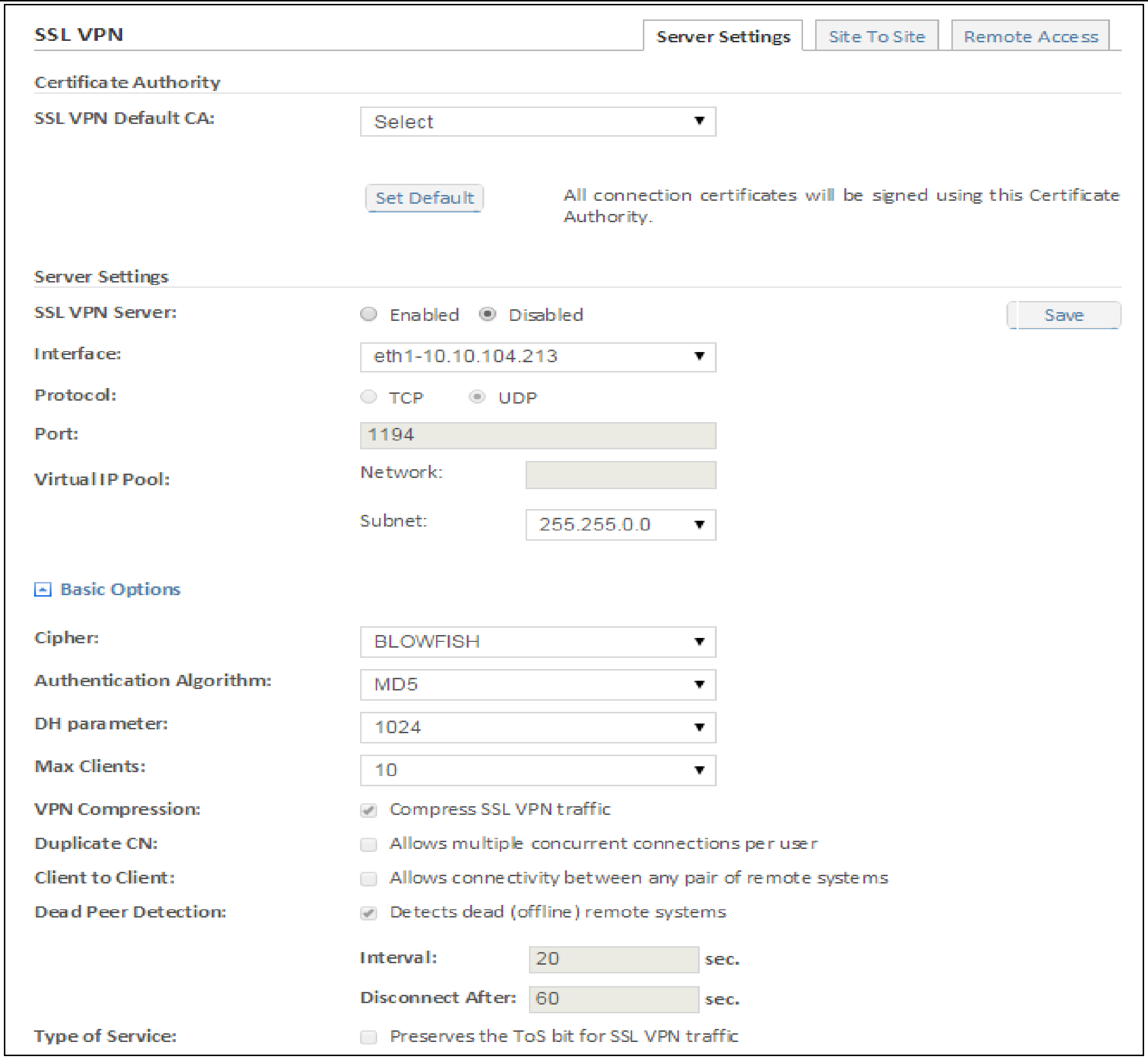
Seqrite Terminator features SSL VPN that allows you to import third party certificates or create self-signed certificates. SSL VPN also provides the following types of connections:

- Site to Site
- Single PC remote connection

Configuring SSL VPN Server Settings

To configure SSL VPN server settings, follow these steps:

1. Log on to Seqrite Terminator **> Settings > SSL VPN**. The following screen appears.



SSL VPN

Certificate Authority

SSL VPN Default CA: Select ▾

All connection certificates will be signed using this Certificate Authority.

Server Settings

SSL VPN Server: ○ Enabled ● Disabled

Interface: eth1-10.10.104.213 ▾

Protocol: ○ TCP ● UDP

Port: 1194

Virtual IP Pool: Network:

Subnet: 255.255.0.0 ▾

⊟ Basic Options

Cipher: BLOWFISH ▾

Authentication Algorithm: MD5 ▾

DH parameter: 1024 ▾

Max Clients: 10 ▾

VPN Compression: ☑ Compress SSL VPN traffic

Duplicate CN: ☐ Allows multiple concurrent connections per user

Client to Client: ☐ Allows connectivity between any pair of remote systems

Dead Peer Detection: ☑ Detects dead (offline) remote systems

Interval: 20 sec.

Disconnect After: 60 sec.

Type of Service: ☐ Preserves the ToS bit for SSL VPN traffic

2. Select a **Certificate Authority** for SSL VPN and set it as default using the **Set Default** button.

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

3. By default the SSL VPN Server is disabled. Select the **Enabled** option to enable the server.

   The following table explains the fields on page:

Field	Description
Interface	Select the Interface from the drop-down list. This is the WAN interface on which the SSL VPN will accept connections.
Protocol	Select the Protocol TCP or UDP protocol as required. • TCP: Select this protocol if remote SSL VPN server is running on TCP.

Field	Description
	• UDP: Select this protocol if remote SSL VPN server is running on UDP
Port	The Port numbers displays the default SSL VPN port.
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**.
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.
Authentication Algorithm	Select the data authentication algorithm for your network.
DH parameter	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.
Max 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 remote systems.
Dead Peer Detection	Select this option if you want Terminator to detect offline remote systems.
Type of Service	Select this option to preserve the ToS bit for SSL VPN traffic.

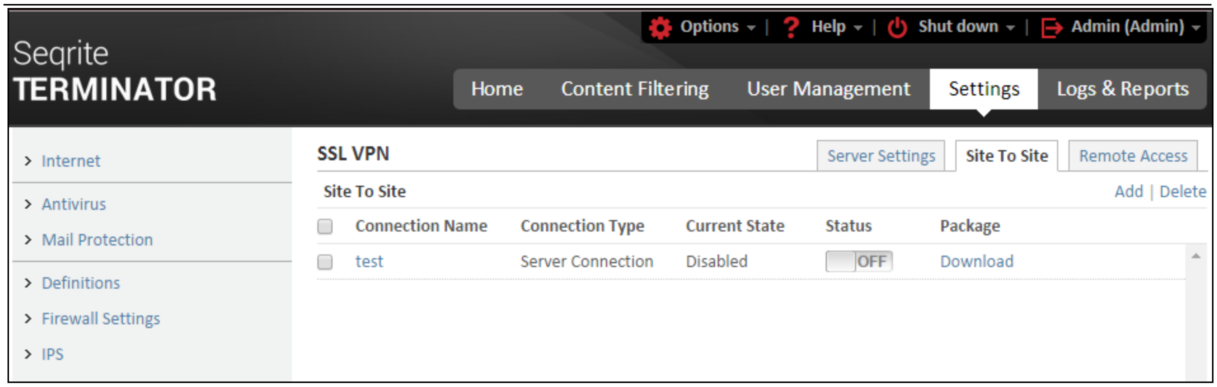
4. Click **Save**.

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.

To add site-to site connections follow the steps given below:

1. Log on to Seqrite Terminator**> Settings> SSL VPN > Site to Site**. The site to site configuration page is displayed.

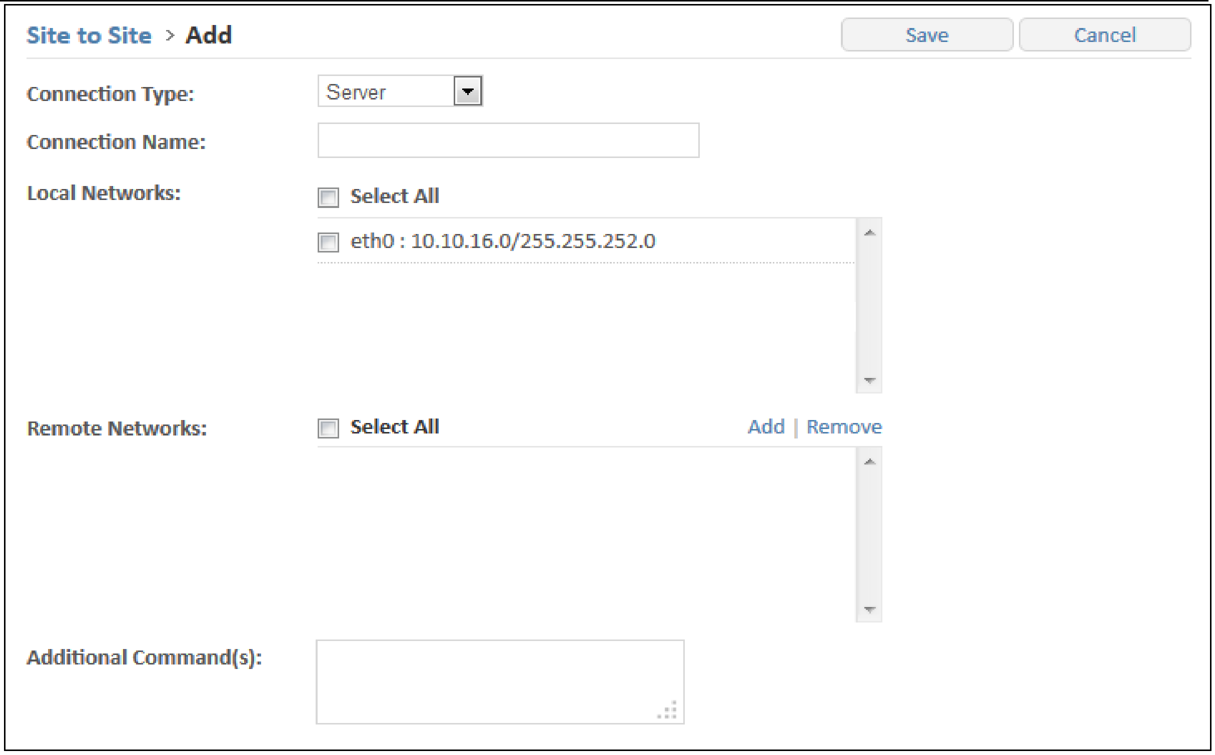


Connection Name	Connection Type	Current State	Status	Package
test	Server Connection	Disabled	OFF	Download

2. Click **Add**. The Site-to Site Add page is displayed.

3. Select the type of connection that you want, whether Server or Client.

   If you select the Server type, the following screen is displayed:



Connection Type: Server

Connection Name:

Local Networks: □ Select All

□ eth0 : 10.10.16.0/255.255.252.0

Remote Networks: □ Select All

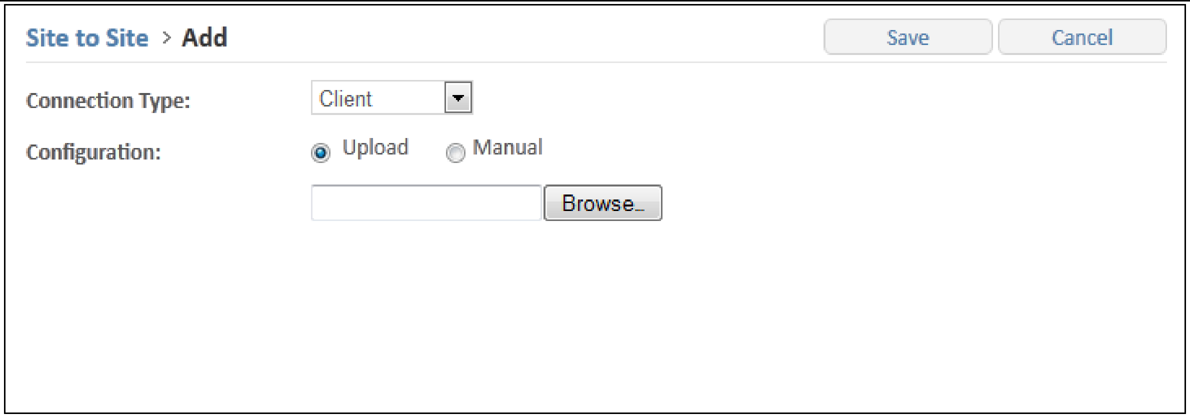
Additional Command(s):

The following table explains the fields on the page:

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 as required. For example: route-gateway 10.10.16.1 ifconfig-push 10.10.16.53 10.10.16.54 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 options are displayed:

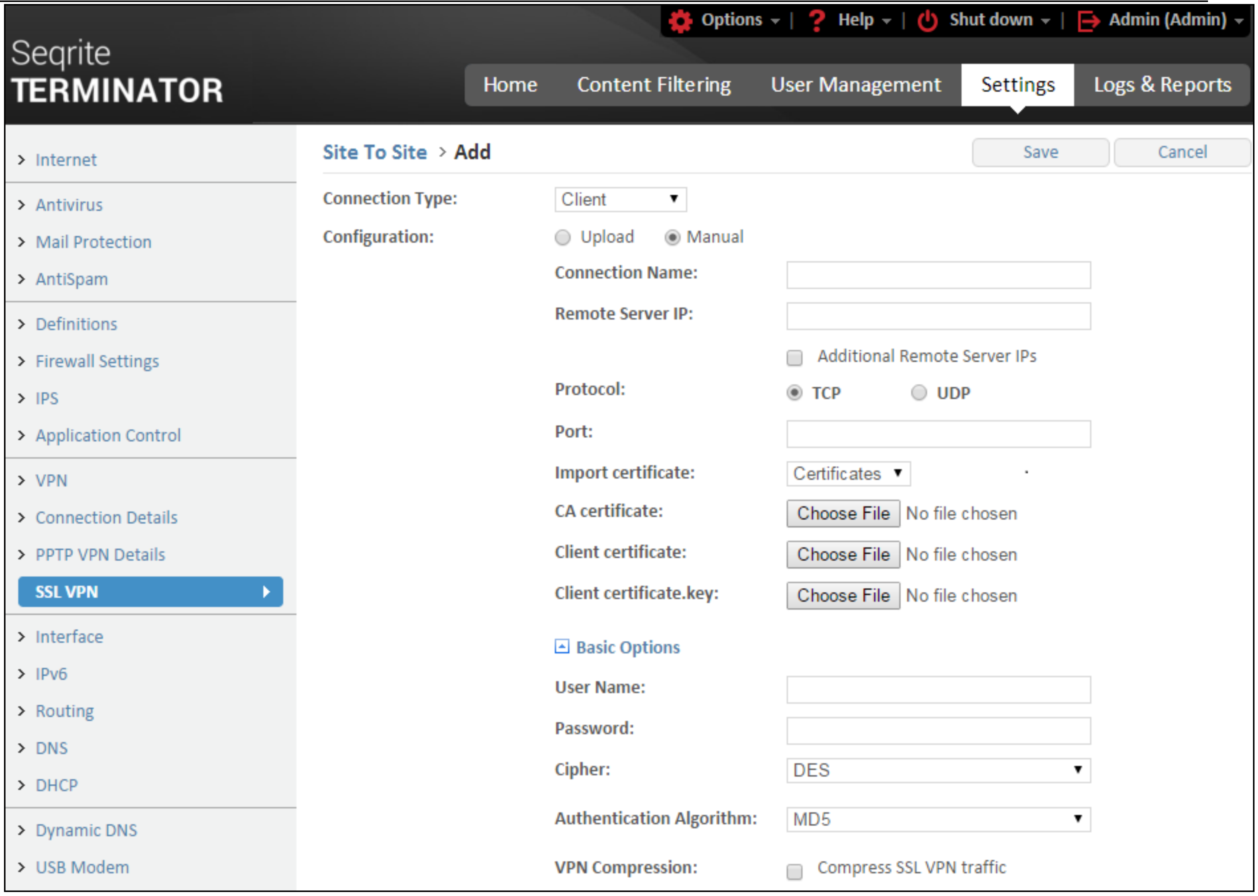


Connection Type: Client

Configuration: ● Upload ○ Manual

5. You can Upload a PKG file or select to manually configure the settings. If you have the PKG file, select **Upload** option. Click **Choose file** to browse the file.

6. If you select the **Manual** option, you must configure the following details:



Site To Site > Add

Connection Type: Client

Configuration: ○ Upload ● Manual

Connection Name:

Remote Server IP:

□ Additional Remote Server IPs

Protocol: ● TCP ○ UDP

Port:

Import certificate: Certificates

CA certificate: Choose File No file chosen

Client certificate: Choose File No file chosen

Client certificate.key: Choose File No file chosen

Basic Options

User Name:

Password:

Cipher: DES

Authentication Algorithm: MD5

VPN Compression: □ Compress SSL VPN traffic

The following table explains the fields:

Field	Description
Connection Name	Enter the name of the connection.
Remote server IP	Enter the IP address of your remote site to which remote SSL VPN Server is bound.
Additional Remote Server IPs	Add additional IPs if your remote SSL VPN Server is bound on multiple IPs.
Protocol	TCP: Select this protocol if remote SSL VPN server is running on TCP. UDP: Select this protocol if remote SSL VPN server is running on UDP.
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.

Field	Description
	PKCS#12: Import certificate in .p12 format and provide the password for file.

7. You can also configure the following **Advanced** options. This setting must match on both sides.

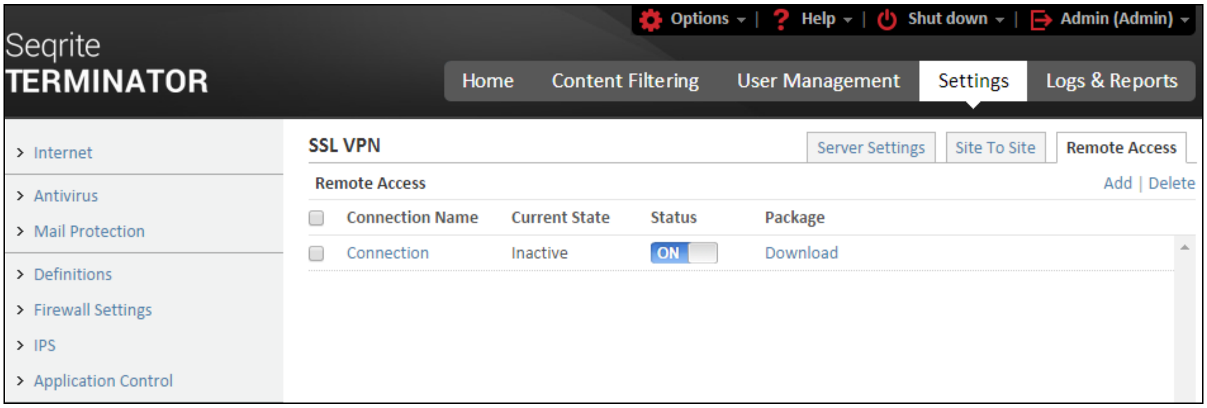
Field	Description
Username	The username provided by the third party SSL VPN server for connection.
Password	The password provided by the third party SSL VPN server for connection.
Cipher	Encrypt packets with cipher algorithm. This setting must match on both sides.
Authentication Algorithm	Authenticate packets with given algorithm. This setting must match on both sides.
VPN Compression	If you want to compress the transmitted data, select the Compress SSL VPN traffic checkbox.

8. Click **Save**.
9. Once 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.
10. 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

To configure Single PC remote access, follow the steps given below:

1. Log on to Seqrite Terminator > **Settings > SSL VPN > Remote Access**. The SSL VPN Remote access connections list is displayed. The current connections are displayed in the list.

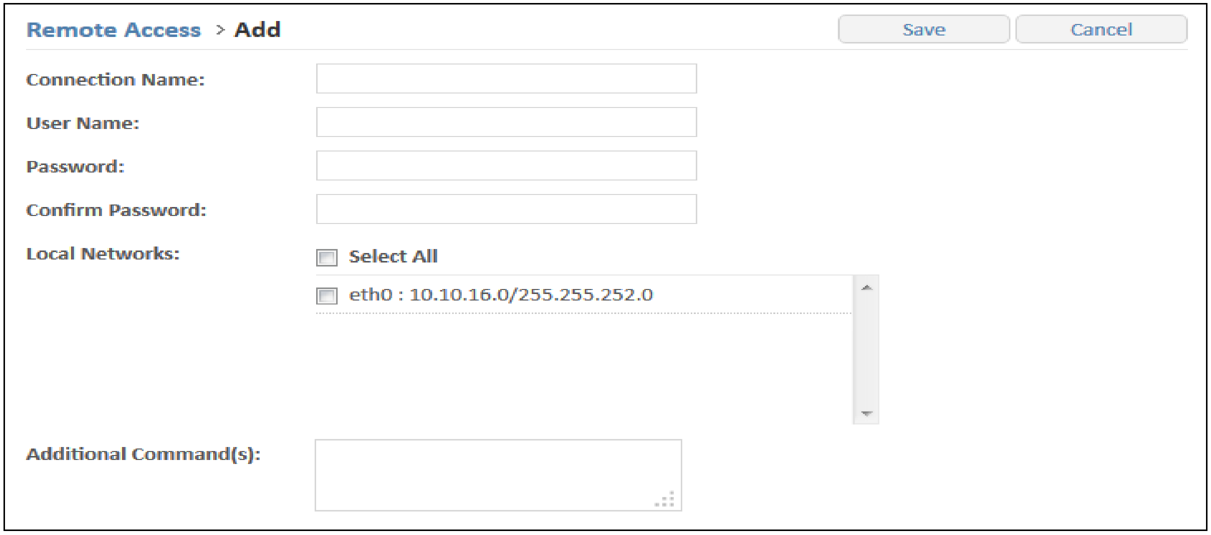


SSL VPN

Remote Access

□	Connection Name	Current State	Status	Package
□	Connection	Inactive	ON	Download

2. Click **Add**. The Remote Access Add configuration page is displayed.



Remote Access > Add

Connection Name:

User Name:

Password:

Confirm Password:

Local Networks: □ Select All

□ eth0 : 10.10.16.0/255.255.252.0

Additional Command(s):

3. Enter the **Connection Name**.

4. Enter the **Username** and **Password** in the designated text boxes. Retype the Password in **Confirm Password** text box. This is used for authentication.

5. Select the **Local networks** that are listed.

6. Add **Additional Commands** if any.

7. Click **Save**.

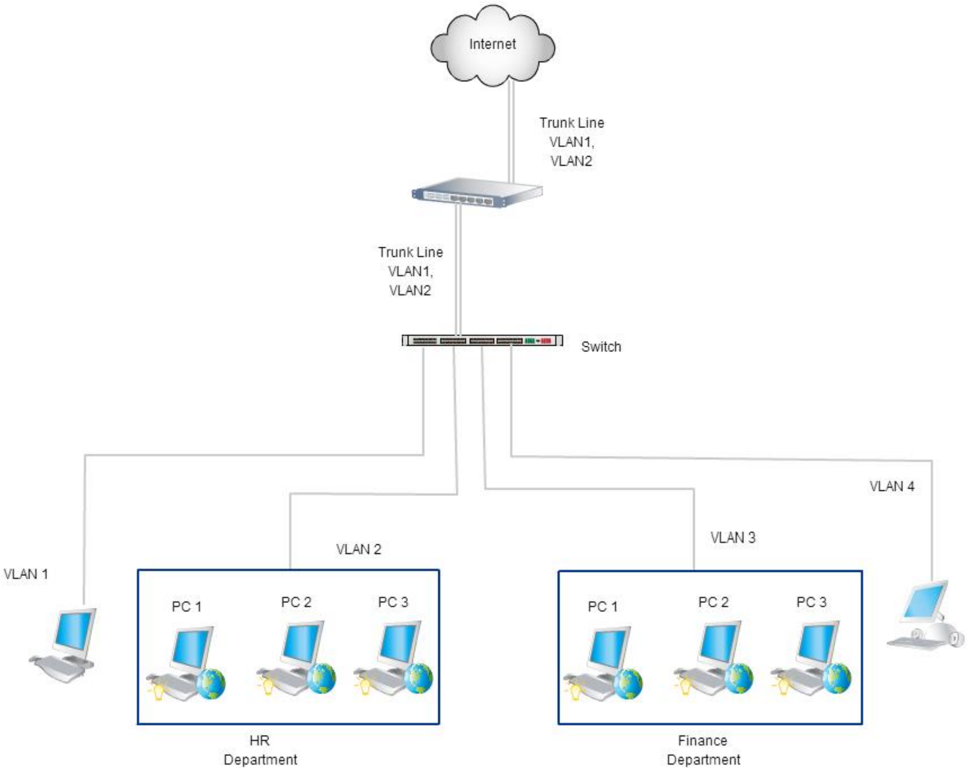
Deleting remote access sites for SSL VPN

1. Log on to Seqrite Terminator> **Settings> SSL VPN > Remote Access**. The SSL VPN Remote access connections list is displayed. The current connections are displayed in the list.

2. Select the SSL VPN connection that you want to delete, click **Delete**.

VLAN

A Virtual Local Area Network (VLAN) is a group of workstations, servers and network devices with same set of requirement 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

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

You can create the following types of VLAN:

VLAN- LAN: For Local Network.

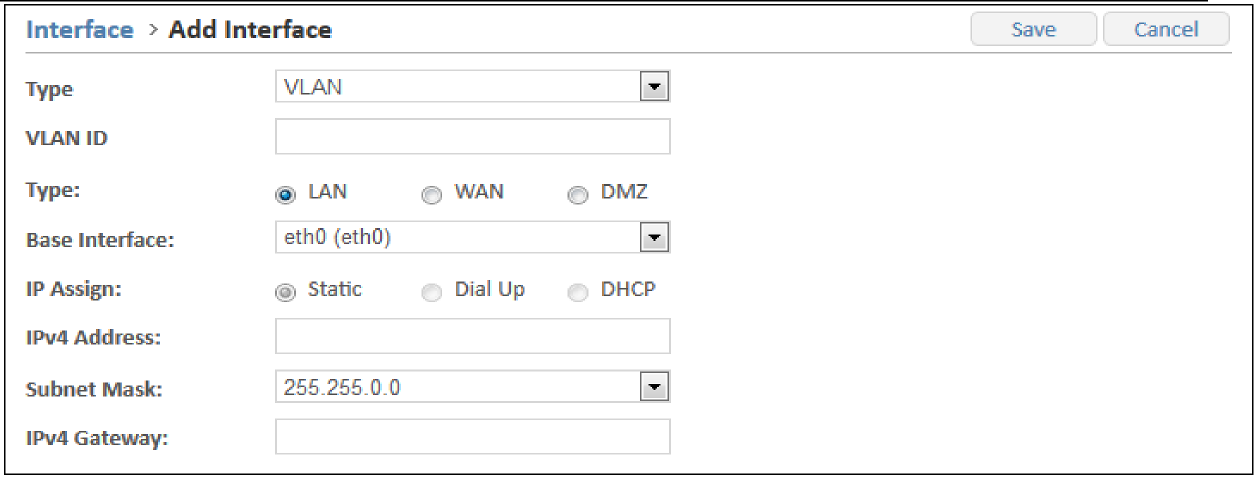
VLAN –WAN: For external network (Internet)/ ISP.

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 the Terminator. The number of ports will be the same that are the default ports depending on the Terminator Model.

To add a VLAN interface follow the steps given below:

1. Log on to Seqrite Terminator > **Settings > Interface**. The Interface details page is displayed.
2. Click **Add**. The following page is displayed.



Type	VLAN
VLAN ID	
Type:	● LAN ○ WAN ○ DMZ
Base Interface:	eth0 (eth0)
IP Assign:	● Static ○ Dial Up ○ DHCP
IPv4 Address:	
Subnet Mask:	255.255.0.0
IPv4 Gateway:	

3. Select the type of Interface as **VLAN**.
4. On selecting VLAN, enter the following details:

   i. Enter the **VLAN ID**. This should be between the ranges 2- 4094.

   ii. Select the **Zone** of operation, whether LAN, WAN, or DMZ.

   iii. Select the **Base Interface** that is the physical port. All the configured and uncofigured network interfaces will be displayed here.

5. Select the type of **IP assignment**, whether Static, Dial up, or DHCP.

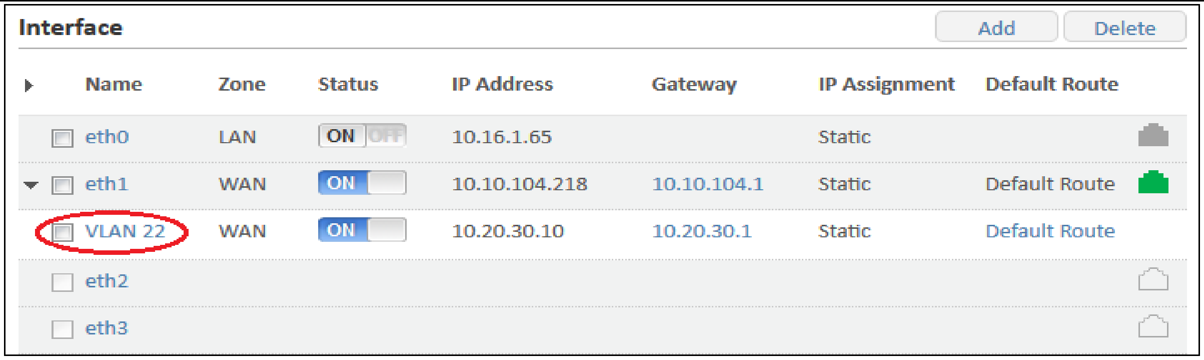
   Note: For LAN and DMZ interface the IP assignment will be only Static.

   i. If you select the IP assignment as Static then you need to enter the IPV4 address and Subnet mask.

   ii. If you select the IP assignment as Dialup then you need to enter the Username and Password provided by your ISP.

6. Click **Save**.

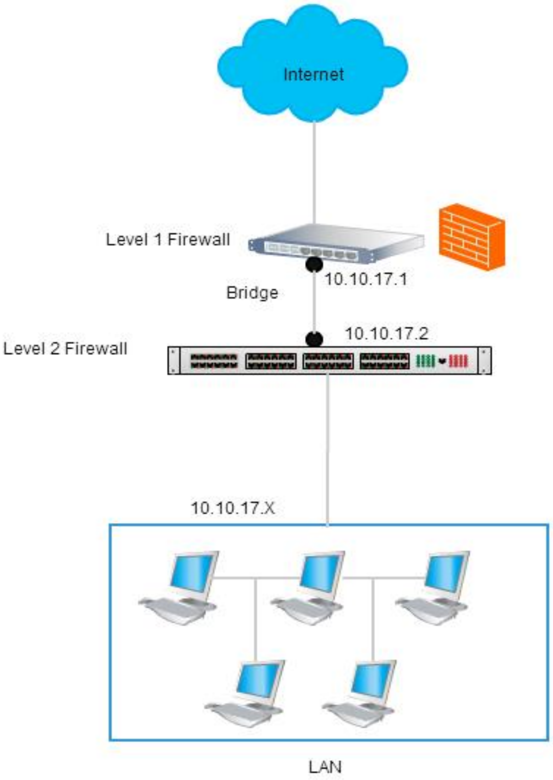
   Note: Every VLAN interface is displayed in interface list as a sub interface of base interface.



Name	Zone	Status	IP Address	Gateway	IP Assignment	Default Route
☐ eth0	LAN	ON OFF	10.16.1.65		Static	
☐ eth1	WAN	ON	10.10.104.218	10.10.104.1	Static	Default Route
☐ VLAN 22	WAN	ON	10.20.30.10	10.20.30.1	Static	Default Route
☐ eth2						
☐ eth3						

Bridge

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

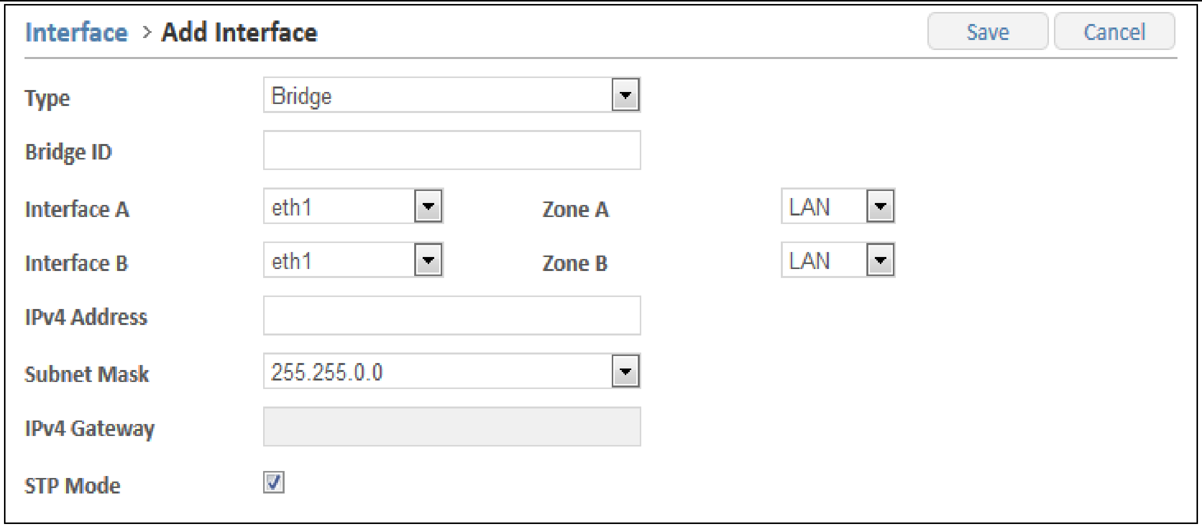


You can use Seqrite Terminator bridge interface as:

- **Transparent gateway:** Seqrite Terminator 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 Terminator device connects to internal network segments i.e. LAN-LAN, LAN-DMZ or DMZ-DMZ bridge.

To add a bridge interface follow the steps given below:

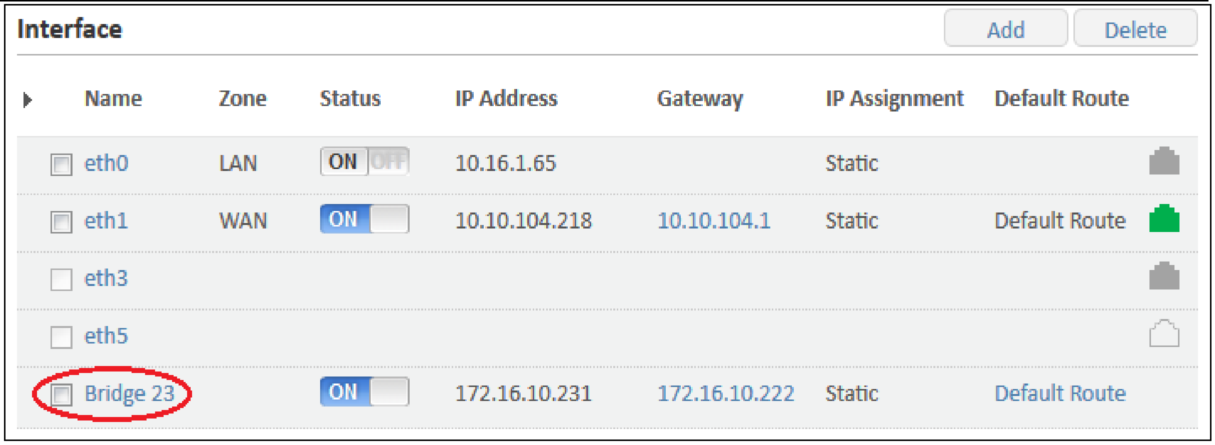
1. Log on to Seqrite Terminator > **Settings > Interface**. The Interface details page is displayed.
2. Click **Add**. The following page is displayed.



Interface > Add Interface

Type	Bridge		
Bridge ID			
Interface A	eth1	Zone A	LAN
Interface B	eth1	Zone B	LAN
IPv4 Address			
Subnet Mask	255.255.0.0		
IPv4 Gateway			
STP Mode	☑		

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



Interface

	Name	Zone	Status	IP Address	Gateway	IP Assignment	Default Route	
□	eth0	LAN	ON OFF	10.16.1.65		Static		
□	eth1	WAN	ON	10.10.104.218	10.10.104.1	Static	Default Route	
□	eth3							
□	eth5							
□	Bridge 23		ON	172.16.10.231	172.16.10.222	Static	Default Route	

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.

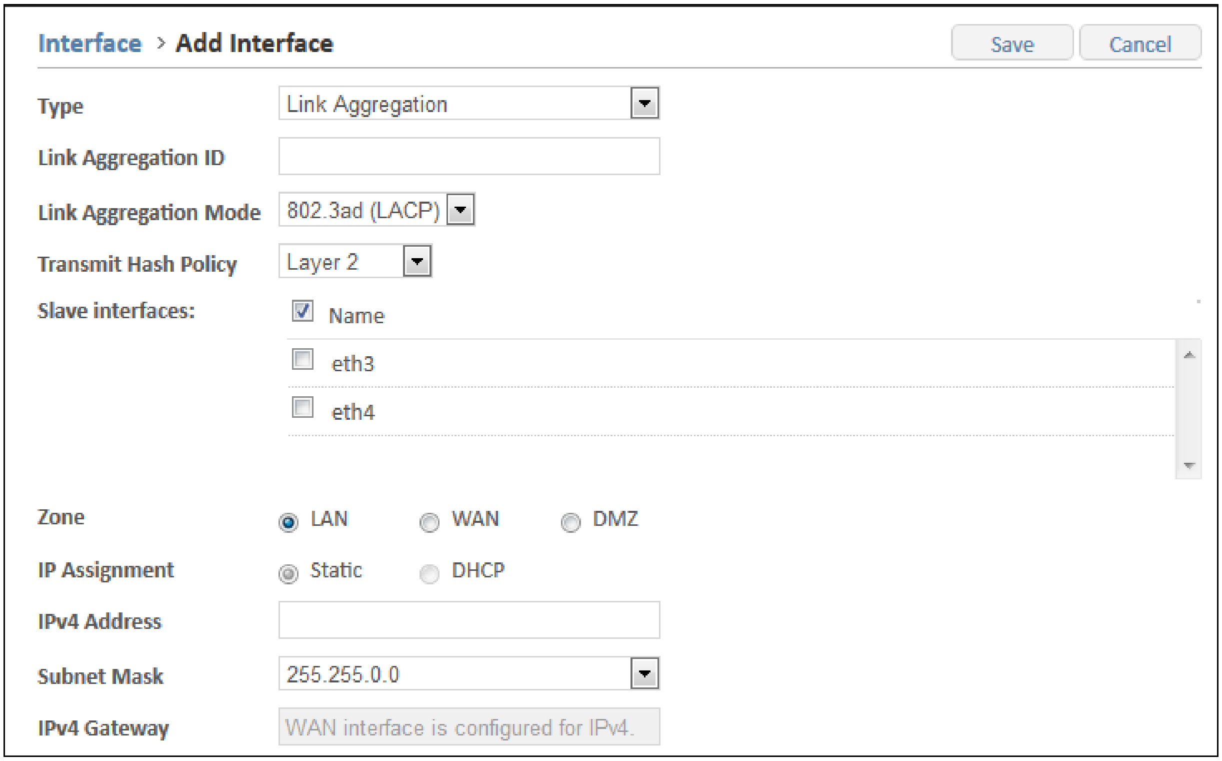
Link Aggregation feature offers the following two benefits:

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.

To create Link Aggregation interface follow the steps given below:

1. Log in to Seqrite Terminator**> Setting> Interface**. The Interface page is displayed.
2. Click **Add**. The Add Interface page is displayed.



Type	Link Aggregation
Link Aggregation ID	
Link Aggregation Mode	802.3ad (LACP)
Transmit Hash Policy	Layer 2
Slave interfaces:	☑ Name □ eth3 □ eth4
Zone	● LAN ○ WAN ○ DMZ
IP Assignment	● Static ○ DHCP
IPv4 Address	
Subnet Mask	255.255.0.0
IPv4 Gateway	WAN interface is configured for IPv4.

Following table explains the fields on page:

Field	Description
Type	Select the interface type as Link aggregation from the dropdown.

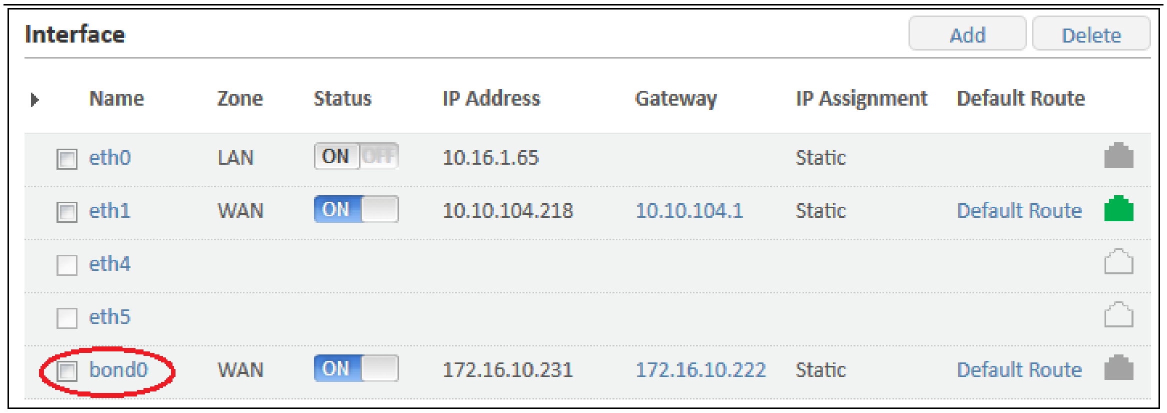
Field	Description
Link Aggregation ID	Enter a Link Aggregation ID. This should be a unique number for identification between the range 0-99.
Link Aggregation Mode	Select the link aggregation mode. Mode specifies bonding policies that will be applied. The following modes of Link Aggregation are available: 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 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

Field	Description
	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 **Save**.

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.



Interface

	Name	Zone	Status	IP Address	Gateway	IP Assignment	Default Route
□	eth0	LAN	ON OFF	10.16.1.65		Static	
□	eth1	WAN	ON	10.10.104.218	10.10.104.1	Static	Default Route
□	eth4						
□	eth5						
□	bond0	WAN	ON	172.16.10.231	172.16.10.222	Static	Default Route

Internet Settings and Exclusion

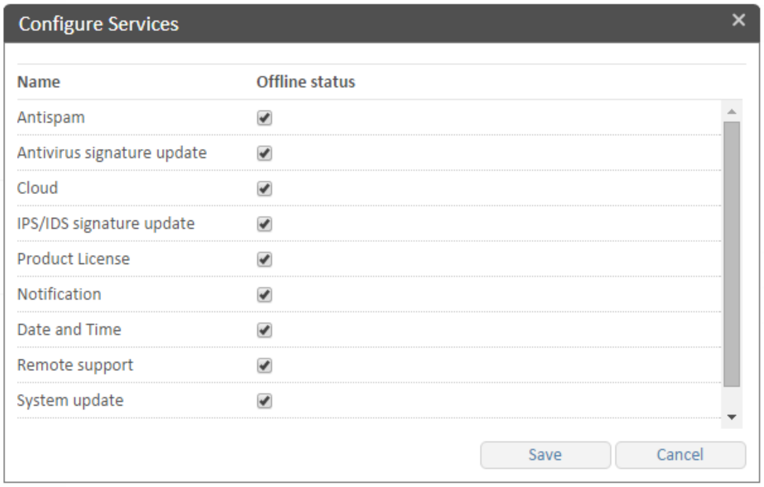
You can control the Internet access for the user. You can give direct access or partial access depending on the designation and requirement of the user. For example, the Director or VP may require direct unfiltered content access, while others can be given access after content filtering. Also, you may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

To configure Internet settings follow the steps given below:

1. Log on to Seqrite Terminator**> Settings**. By default, the Internet settings page is displayed. The Internet settings page displays the IP address and the ports of the Terminator server.

The following table described the fields on the page:

Field	Description
Direct Internet Access	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.
Direct Accessible 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 URLs with Invalid Certificates	Certain certificate errors may occur for an internal site with self-signed certificates or for an internal domain name for a site differing from its public certificate name. Click on Add/Remove to Exclude/Remove such domains. Note: Ignoring certificate errors is a security flaw. Excluding it in a shared proxy is an extremely dangerous action. URLs with invalid certificates should not be excluded for domains where you are not an authorized owner (in such case fix the certificate problem before excluding it).
Allowed Normal Traffic	Use this section to add the port numbers for open access. The Web sites which are running on these ports are allowed to be accessed by the user. Default HTTP port 80 is already added and cannot be deleted.
Allowed Secured Traffic	Use this section to add the port number for secured traffic. The secured Web site which are running on these ports are allowed to be accessed by the user. Default HTTPS port 443 is a default port and cannot be deleted.
Bypass Secured Traffic	If you select this option, all HTTPS Web sites will be directly accessible without any monitoring and control. Note: You must not configure proxy in the browser.
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 Terminator products deployed in the network to be silently updated.
Include X-Forwarded-For header information	To provide extra privacy to the end user, the Terminator can be configured to remove the 'X-Forwarded-For' HTTP header. By default this option is enabled in the Terminator. Disabling this option removes the end user's host IP information from the HTTP headers in

Field	Description
	the outgoing requests. You may need to keep this option enabled especially in case of bridge mode if you are using an existing firewall.
Device 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. On clicking the **Configure Services** button, a list of services displayed.  Configure Services Name — Offline status Antispam ☑ Antivirus signature update ☑ Cloud ☑ IPS/IDS signature update ☑ Product License ☑ Notification ☑ Date and Time ☑ Remote support ☑ System update ☑ Select the services that you want to be offline and click **Save**. Note: These services will be offline only if the Device offline mode is selected.
Enable Device Internet Quota	Using this option you can enable internet quota for the Terminator. Select this option and configure the internet policy that you would like to apply for the Terminator. Click **Configure Setting** to create the device Internet quota policy. (See Internet Quota for more details). Note: This Quota policy has higher weightage than user / group quota policy. When the device internet quota is fully consumed, all the users will be logged out and internet access will be denied.

2. Click **Save**.

   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.

Chapter

6

Identity Management/ Users and Groups

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:

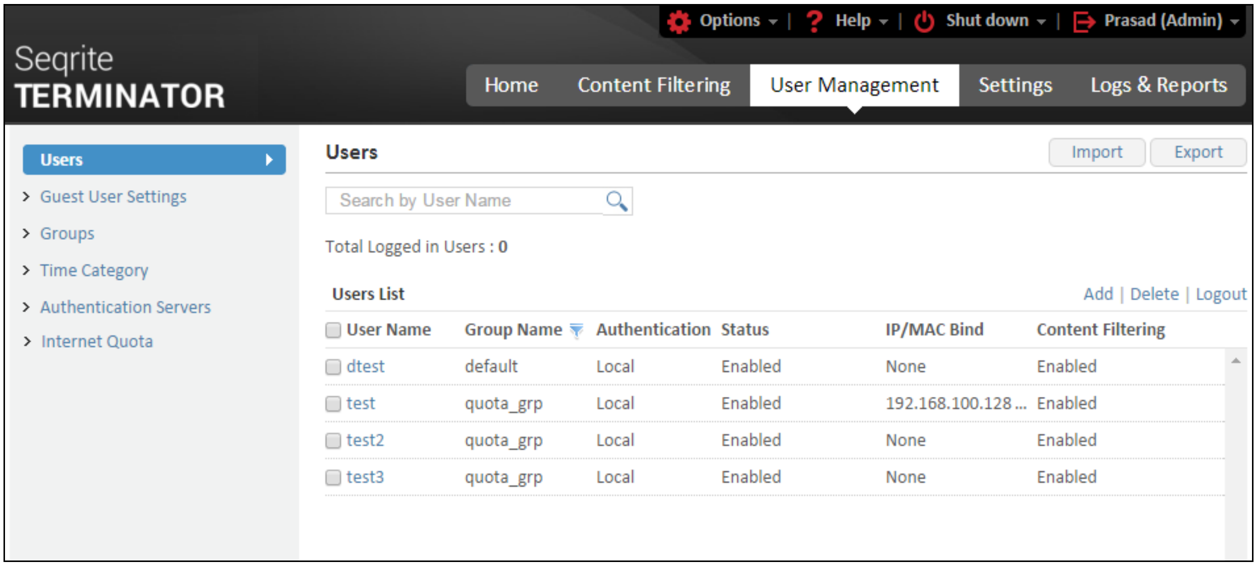
- Users
- Guest User Settings
- Groups
- Time category
- Authentication servers
- Internet Quota

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

User Management

The Users feature 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. The Users page displays the details of the users, such as user name, group name, authentication, login status, IP/MAC bind details and content filtering status. This page also displays the count of total number of users that are logged in.

Note: The Name wise users cannot browse Internet or access mails if they are not logged in.



Users

Total Logged in Users : 0

Users List

User Name	Group Name	Authentication	Status	IP/MAC Bind	Content Filtering
dtest	default	Local	Enabled	None	Enabled
test	quota_grp	Local	Enabled	192.168.100.128 ...	Enabled
test2	quota_grp	Local	Enabled	None	Enabled
test3	quota_grp	Local	Enabled	None	Enabled

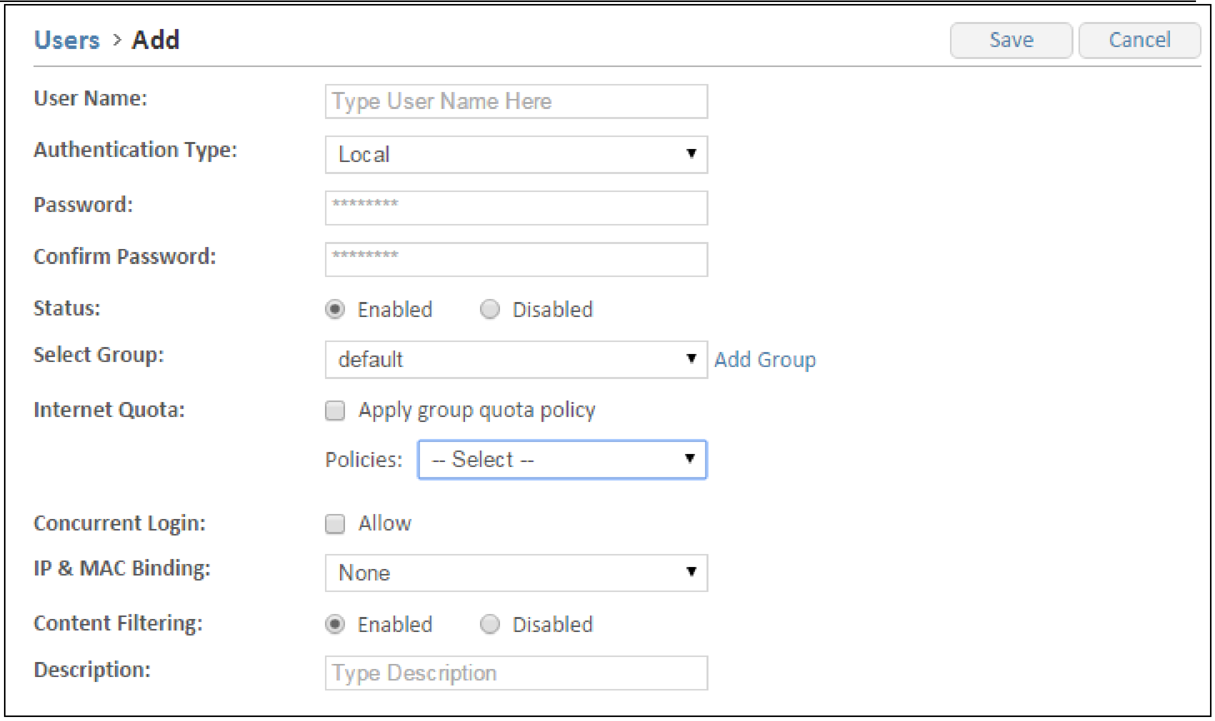
The status field has the following options:

Field	Description
Enabled	This status indicates that the user is in enabled state and can login to Terminator to access Internet.
Disabled	This status indicates that the user is disabled by an administrator and cannot login to Terminator to access Internet.
Logged In	This status indicates that the user is currently logged in. Administrator can forcefully logout a user, by selecting the user from Users List and clicking the **Logout** button.

Adding a user

To add a new user follow the steps given below:

1. Log on to Seqrite Terminator **> User Management>Users**. The Users management page is displayed.
2. Click **Add** on upper right corner. The **Add Users** screen is displayed.



Users > Add

Save | Cancel

User Name:	Type User Name Here
Authentication Type:	Local ▾
Password:	********
Confirm Password:	********
Status:	● Enabled ○ Disabled
Select Group:	default ▾ Add Group
Internet Quota:	□ Apply group quota policy
	Policies: -- Select -- ▾
Concurrent Login:	□ Allow
IP & MAC Binding:	None ▾
Content Filtering:	● Enabled ○ Disabled
Description:	Type Description

The table below explains the fields on page:

Field	Description
User name	Enter the **User name**.
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 Terminator. If the user is authenticated through Authentication Server then, the username must be identical to the username on the Authentication Server.
Password	Enter a password. Password should be alphanumeric and between 6 to 20 characters in length and has at least one special character.
Confirm Password	Re-enter the password for confirmation.
Status	Enabled: The user can authenticate and login to Terminator and access Internet. Disabled: The user cannot login to Terminator and cannot access the Internet.
Select Group	Select the group that you want to assign to the user and apply the policies. Note: A group is available only if it is created earlier.
Internet Quota	You can select the option to apply the Same internet quota policy as

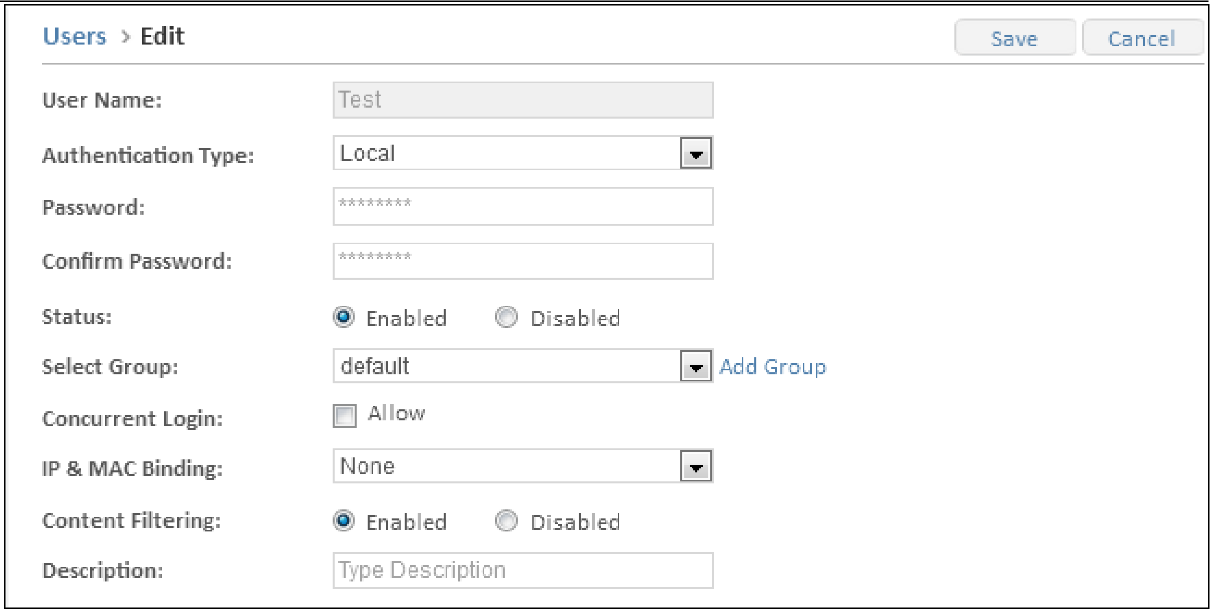
Field	Description
	that of the selected group. You can clear this option and select an individual Internet Quota policy from the given dropdown.
Concurrent Login	Use this option to allow users to simultaneously login from multiple system. You can set the maximum number of concurrent login that can be allowed to be Unlimited or Custom. If you select the custom option, then you can set a value for the maximum number of concurrent login.
IP and MAC binding	Binds the User Name to a particular IP address or MAC address or both as configured. 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.
Content Filtering	If set to enabled, content is filtered as configured for the group assigned to the User. If set to disabled, no content filtering rules are applied for the user.
Description	Enter description about the user.

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

Editing a User

To edit a user follow the steps given below:

1. Log on to Seqrite Terminator **> User Management > Users**.
2. Click on the **User Name** in the list given on the Users page. The following screen is displayed.



User Name: Test

Authentication Type: Local

Password: ********

Confirm Password: ********

Status: ● Enabled ○ Disabled

Select Group: default

Concurrent Login: □ Allow

IP & MAC Binding: None

Content Filtering: ● Enabled ○ Disabled

Description: Type Description

3. Make the required changes in the User details and 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 100MB internet usage and the user has used 70MB of data. While editing if a new policy is selected, then resetting the previous data usage will clear the 70 MB usage.

Deleting users

To delete a User follow the steps given below:

1. Log on to Seqrite Terminator > **User Management> Users**. The Users management page is displayed.
2. This page displays the list of the users with the User name, Group name, Authentication, Status, IP MAC binding status, and Content filtering status.
3. To delete a user, select the user and click **Delete**. The selected user is deleted.

   Note: You can also select multiple users for deletion.

Logging out a user by force

To log out a user by force follow the steps given below:

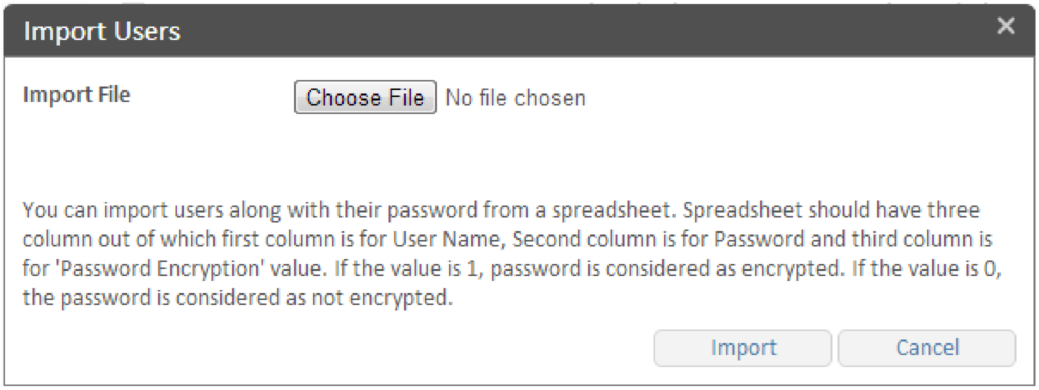
1. Log on to Seqrite Terminator> **User Management> Users**. The Users management page is displayed.
2. This page displays the list of the users with the User name, Group name, Authentication, Status, IP MAC binding status, Content filtering whether enabled and email ID if created.
3. Select the User name and click **Logout**. The user is logged out of the network.

Note: You can also select multiple users for logging out by force.

Importing users

You can add users by importing the details from an excel sheet. To import users follow the steps given below:

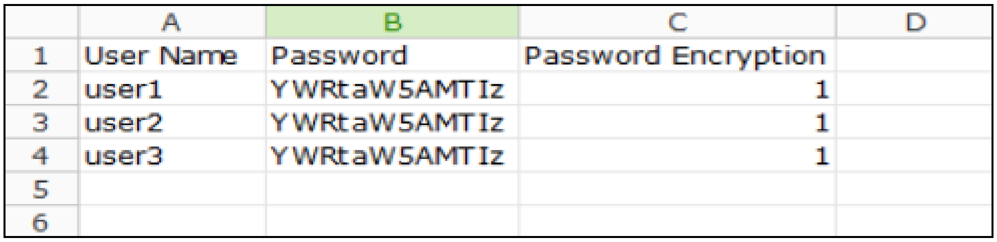
1. Log on to Seqrite Terminator> **User Management> Users**. The Users management page is displayed.
2. This page displays the list of the users with the User name, Group name, Authentication, Status, IP MAC binding status, and Content filtering status.
3. Click **Import**, the Import Users dialog box is displayed.



You can import users along with their password from a spreadsheet. Spreadsheet should have three column out of which first column is for User Name, Second column is for Password and third column is for 'Password Encryption' value. If the value is 1, password is considered as encrypted. If the value is 0, the password is considered as not encrypted.

4. Click **Choose file** to browse the excel file containing the user details.

Note: Your spreadsheet should contain three columns. First column should be for **User Name**, second for **Password**, and third for **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.



	A	B	C	D
1	User Name	Password	Password Encryption	
2	user1	YWRtaW5AMTIz	1	
3	user2	YWRtaW5AMTIz	1	
4	user3	YWRtaW5AMTIz	1	
5				
6				

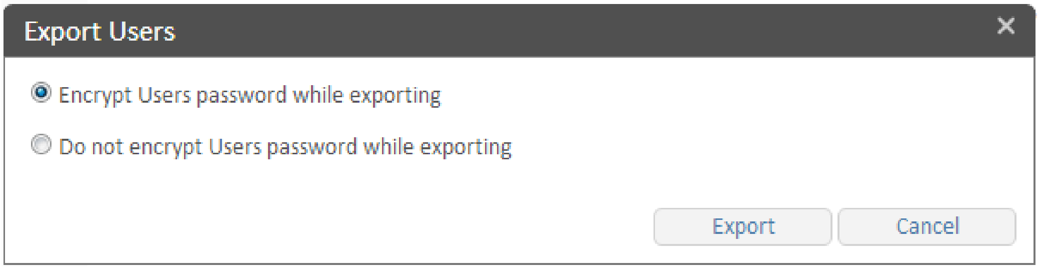
5. Click **Import**. The Import Users dialog box displays a message about the successful addition of users. These users will be listed in the Users list.

Exporting users

To export user details to an excel sheet follow the steps given below:

1. Log on to Seqrite Terminator**> User Management > Users**. The Users management page is displayed by default.

2. This page displays the list of the users with the User name, Group name, Authentication, Status, IP MAC binding status, and Content filtering status.
3. Select the users whose details you want to export to excel sheet, click **Export**. The Export user dialog box is displayed.



Export Users

● Encrypt Users password while exporting

○ Do not encrypt Users password while exporting

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

Guest User Settings

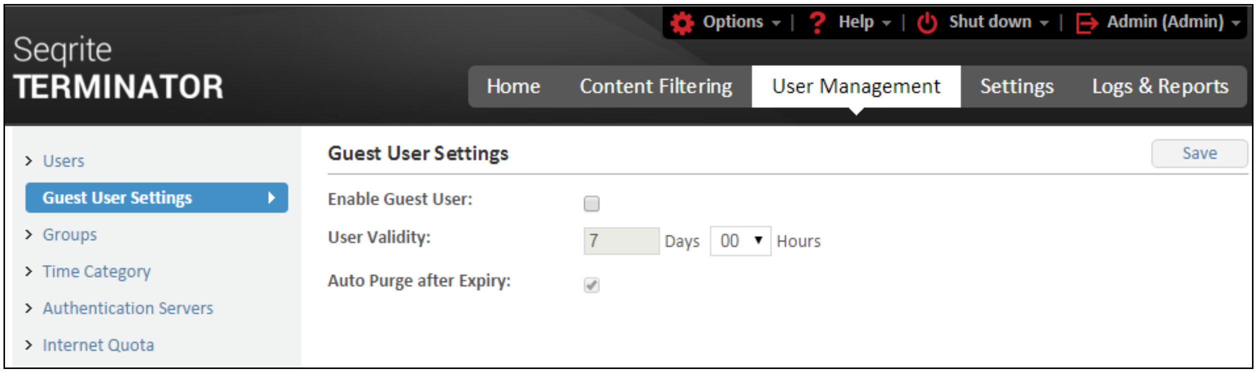
A Guest User is a non-registered user who can be given default set of permissions to access the Internet for a particular time duration.

The Guest user section in Terminator allows you to configure general parameters to provide Internet access for a guest user. After the validity 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.

To configure the settings, follow these steps given below:

1. Log on to Seqrite Terminator **> User Management > Guest Users Settings**. The following screen will be displayed.



Guest User Settings

Enable Guest User: □

User Validity: 7 Days 00 Hours

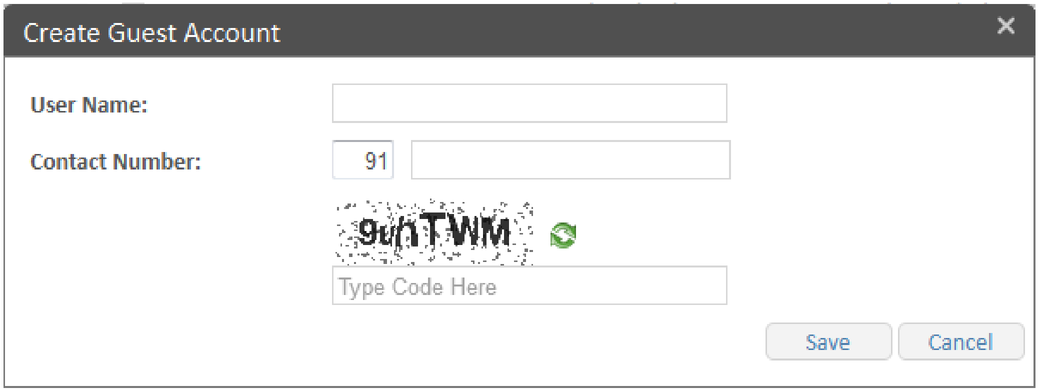
Auto Purge after Expiry: ☑

2. The following table explains the configuration options:

Field	Description

Enable Guest User	Select this option to enable guest user registration on the Terminator
User Validity	Specify guest user validity. On expiry of user validity, guest user will not be allowed to access Internet.
Auto Purge after Expiry	Select this option to enable automatic purging (automatic deletion) of guest user details on expiry of user validity.

3. Once you select the **Enable Guest User** option, **Create Guest Account** link will be displayed on the user login page.
4. Clicking on the **Create Guest Account** link, the following screen will be displayed.



Create Guest Account

User Name:

Contact Number: 91

5. Enter the required details and click **Save**.

   Note: Guest users will be placed in a predefined group named 'Guest'. Guest users will not be moved in other group and vice versa.

   After successful registration, guest user will receive the SMS of credentials and a link for login. Clicking the link will automatically log you in Terminator without entering the credentials.

Group Management

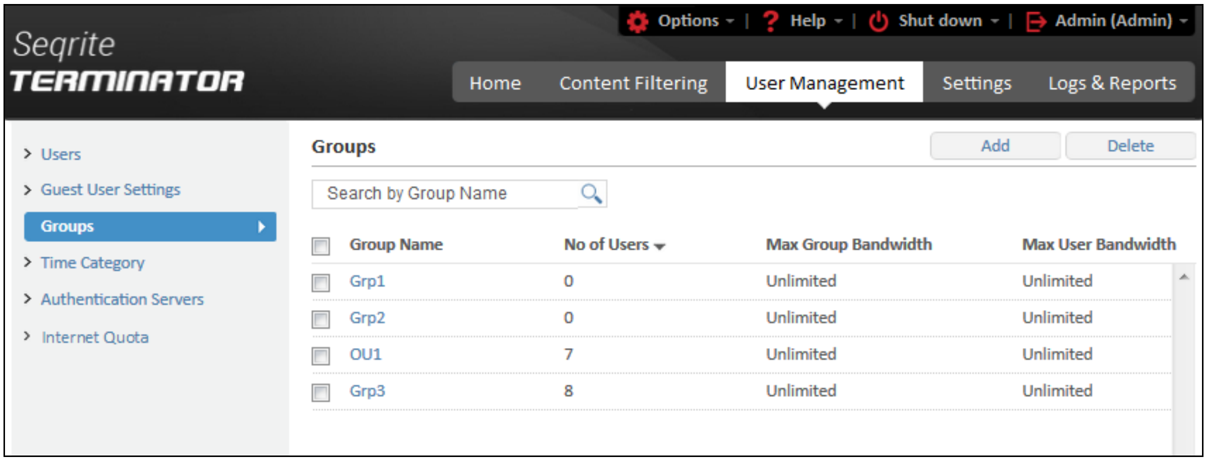
Group is a collection of users that have same policies for accessing Internet. Using the User Management section you can perform the following functions on a Groups.

- 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.

Adding a group

To add a group:

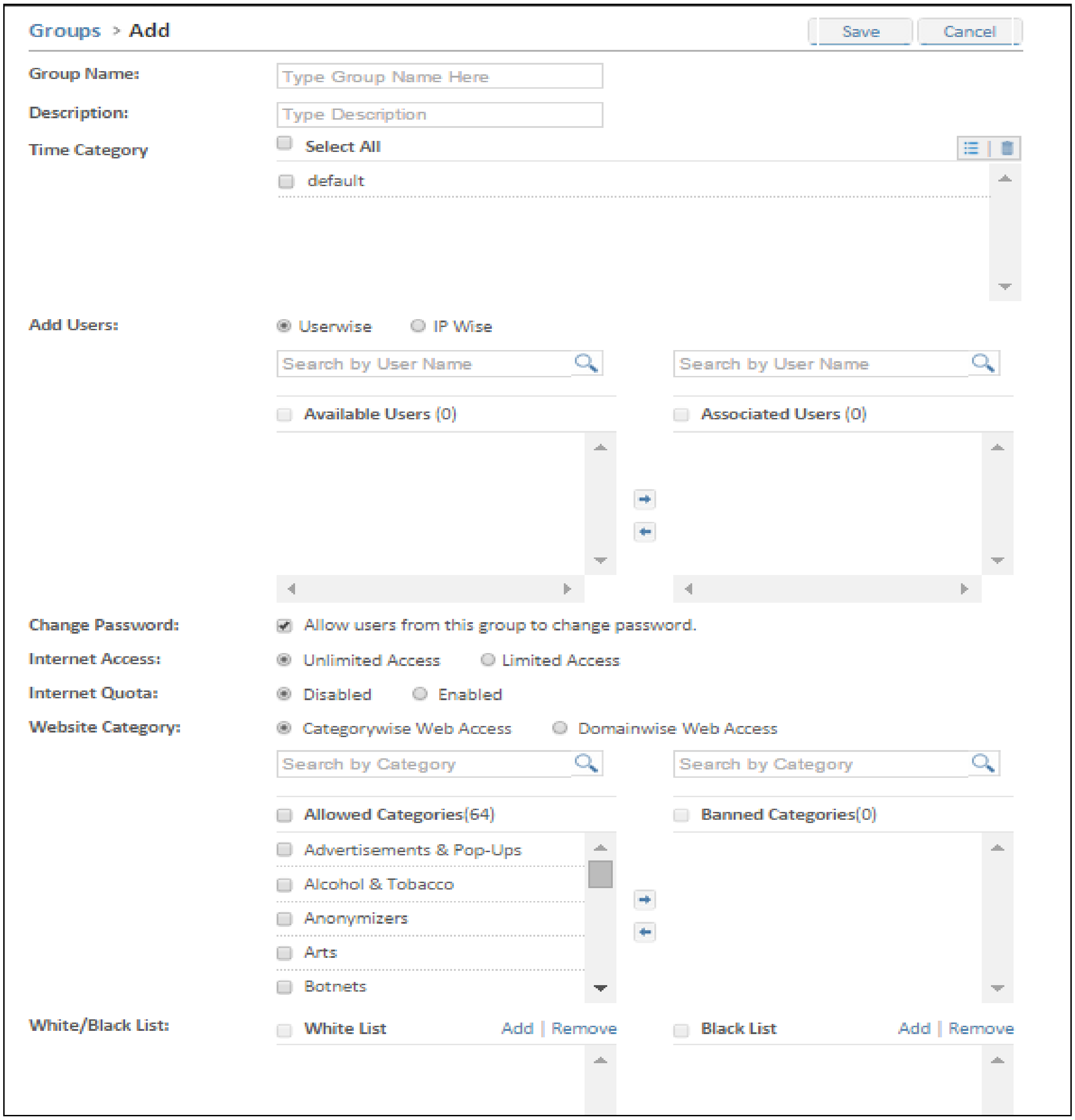
1. Log on to Seqrite Terminator**> User Management > Groups**. The Groups page is displayed with details of groups such as Group name, number of users, Max Group Bandwidth configured, and Max User Bandwidth.



Groups

□	Group Name	No of Users	Max Group Bandwidth	Max User Bandwidth
□	Grp1	0	Unlimited	Unlimited
□	Grp2	0	Unlimited	Unlimited
□	OU1	7	Unlimited	Unlimited
□	Grp3	8	Unlimited	Unlimited

2. Click **Add**.



Group Name: Type Group Name Here

Description: Type Description

Time Category: □ Select All

□ default

Add Users: ● Userwise ○ IP Wise

Search by User Name | Search by User Name

□ Available Users (0) | □ Associated Users (0)

Change Password: ☑ Allow users from this group to change password.

Internet Access: ● Unlimited Access ○ Limited Access

Internet Quota: ● Disabled ○ Enabled

Website Category: ● Categorywise Web Access ○ Domainwise Web Access

Search by Category | Search by Category

□ Allowed Categories(64) | □ Banned Categories(0)

□ Advertisements & Pop-Ups
□ Alcohol & Tobacco
□ Anonymizers
□ Arts
□ Botnets

White/Black List: □ White List Add | Remove   □ Black List Add | Remove

The table below explains the fields on the page:

Field	Description
Group Name	Enter the Group name. Note: You cannot use reserved words and special characters as Group Names
Description	Add a description for the group.
Time Category	Select a Time category for the group. It is the time period for which the User will get Internet access. You can select multiple time category. (See Time Category for more details.)
Add Users	**User wise**: If you select to add users User wise a list of Available Users is displayed. Select the users under Available users and click the right arrow

Field	Description
	to move the selected users to the Associated User lists. The users will be associated to the group and the group policies will be applied. You can select all the users in the Available Users list and move them under Associated Users. One user can be assigned to one group. If a user is already associated to any other group then that user's name will not be displayed in Available User list.
	IP wise: If you select IP wise, you have to enter the following details. Click **Add**, enter the specified IP address of user and click **Save**. For single IP address same IP should be entered in Start and End IP. To define a range of IPs add the IP addresses in *Starting IP address*, the *End IP address*. Click **Save**. Use the **Remove** option to remove any IP address range that is not in use.
Change Password	This option is displayed only for User wise option. Use this option to enable whether the users from the group are allowed to change their passwords.
Internet Access	**Unlimited**: If you select Unlimited, the user can browse the Internet with no limit on browsing. **Limited Access**: If you select Limited Access, the user can browse only as per the limit configured. Accordingly you must configure the following sub-options: Group and user bandwidth in KB/Second **Maximum Group Bandwidth**: This is the maximum bandwidth that is available to the users (cumulative) in this group. Use this to restrict the bandwidth availability for a group. **Maximum User Bandwidth**: This is the maximum bandwidth that is available to each user in this group. Use this to restrict the bandwidth availability for users in a group. **Surfing time** can be set to Unlimited or limited to specified hours for each user.
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.
Website Category	**Category wise**: If you select this option, the user can browse Web sites only from allowed categories. You have the following sub-options: Select the categories from the **Allowed Categories** and move them to the **Banned Categories** list and visa-versa using the arrow head buttons between the lists. Use the **Search by Category** search box to search for Web site categories.

Field	Description
	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 blocked.
White List/Black List	White List: The White list is a list of trusted Web sites that user can access safely. Use the **Add** button to add a Web site to the White List. To remove a Web site from the White List, select the Web site and click **Remove**.
	Black List: The Black List is a list of untrusted Web sites that can be dangerous if accessed. Use the **Add** button to add a Web site to the Black List. To remove a Web site from the Black List, select the Web site and click **Remove**.

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

Edit Group

To edit a group follow the steps given below:

1. Log on to Seqrite Terminator **> User Management > Groups**.
2. Click on the **Group Name** in the list given on the Groups page. The edit group page is displayed.
3. Make the required changes in the Group details and click **Save**.

   Note: Group name cannot be changed while editing a group.

   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 100MB internet usage and the user has used 70MB 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

To delete a group follow the steps given below:

1. Log on to Seqrite Terminator **> User Management> Groups**. The Groups page is displayed with details of groups such as number of users, Max Group Bandwidth utilized, and Max User Bandwidth.

2. Select the group that you want to delete and click **Delete** 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.

Searching for groups

To search for a group follow the steps given below:

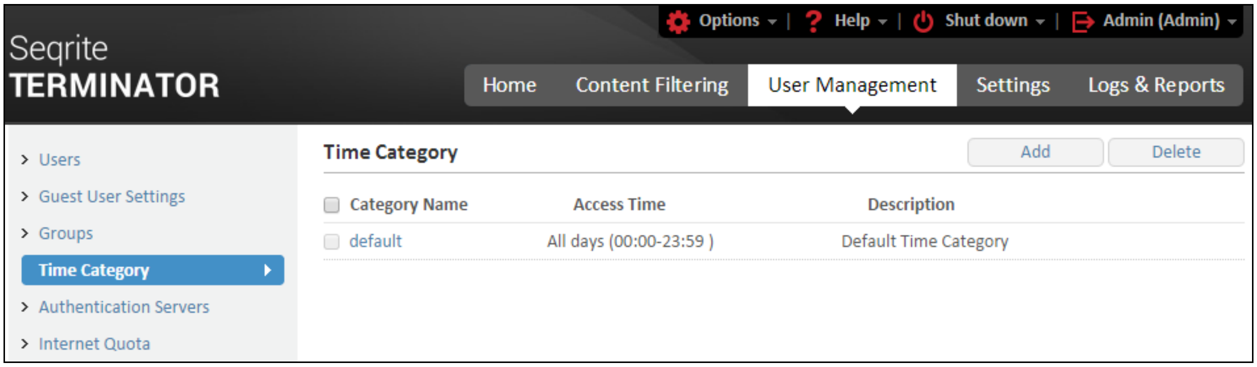
1. Log on to Seqrite Terminator **> User Management > Groups**. The Groups page is displayed with details of groups such as number of users, Max Group Bandwidth utilized, and Max User Bandwidth.
2. In the **Search by Group name** text box, enter the name of the group that you want to look up. For e.g. Default. The group is automatically located and displayed, the other groups are excluded from the list.

Time Category

The time category helps to provide a defined Internet surfing time to users and groups. All available time categories are displayed along with their details, such as, Access Time and description of various categories.

To create a time category, follow the steps given below:

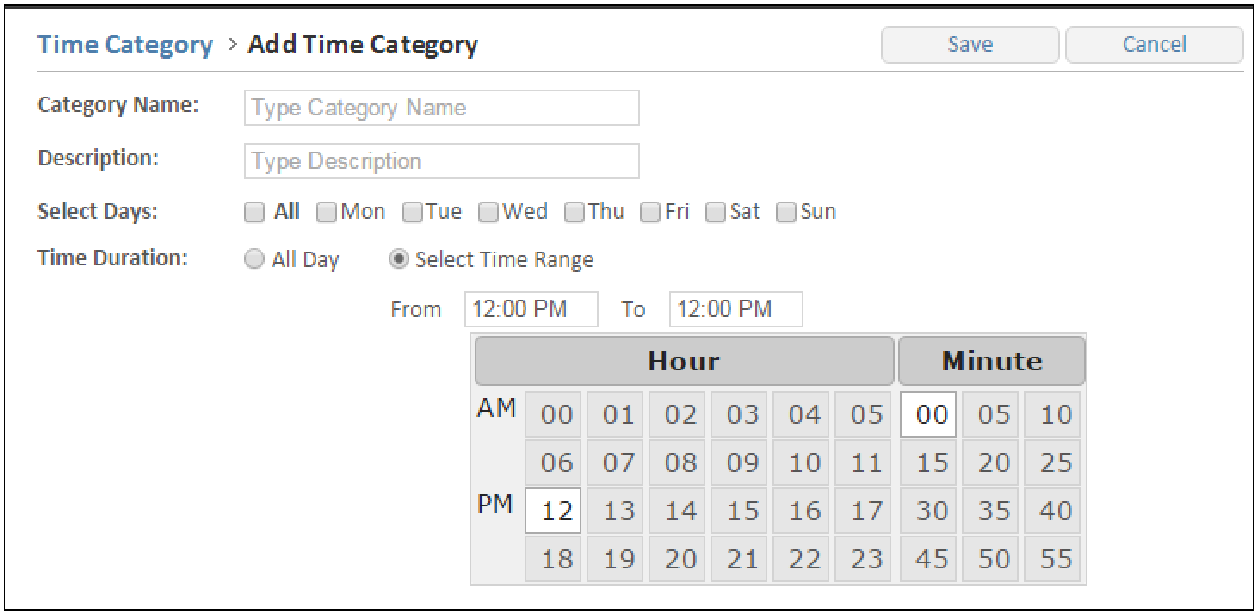
1. Log in to Seqrite Terminator> **User Management**> **Time Category**.



Time Category

□ Category Name	Access Time	Description
□ default	All days (00:00-23:59)	Default Time Category

2. Click **Add** on the right hand side. The Add Time Category page is displayed.



Time Category > Add Time Category

Category Name: Type Category Name

Description: Type Description

Select Days: □ All □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time Duration: ○ All Day ● Select Time Range

From 12:00 PM To 12:00 PM

	Hour						Minute		
AM	00	01	02	03	04	05	00	05	10
	06	07	08	09	10	11	15	20	25
PM	12	13	14	15	16	17	30	35	40
	18	19	20	21	22	23	45	50	55

3. Enter **Category Name** and **Description,** select **Days** and **Time Duration**.
4. 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 LDAP or Active Directory for various groups and users in your network with the Seqrite Terminator. You can also configure the synchronization cycle for Seqrite Terminator to synchronize with the Authentication servers.

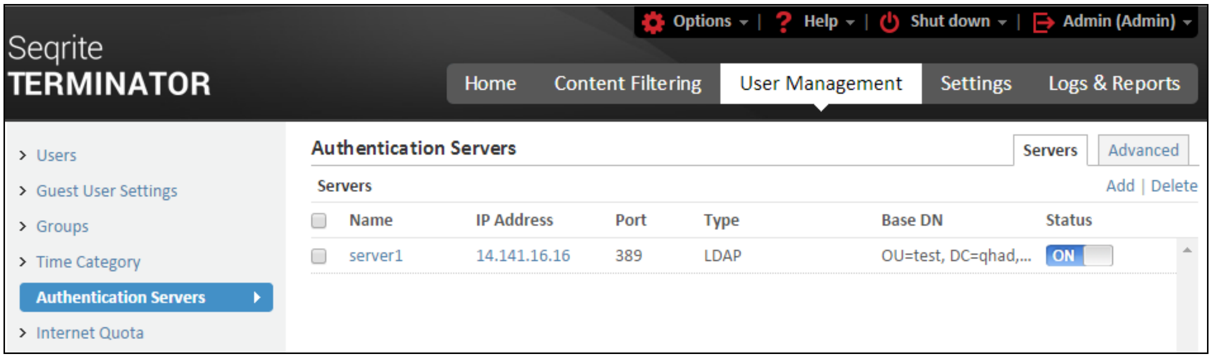
You can perform the following functions under this feature:

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

Adding a new server

To add an authentication server follow the steps given below:

1. Log on to Seqrite Terminator**> 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.

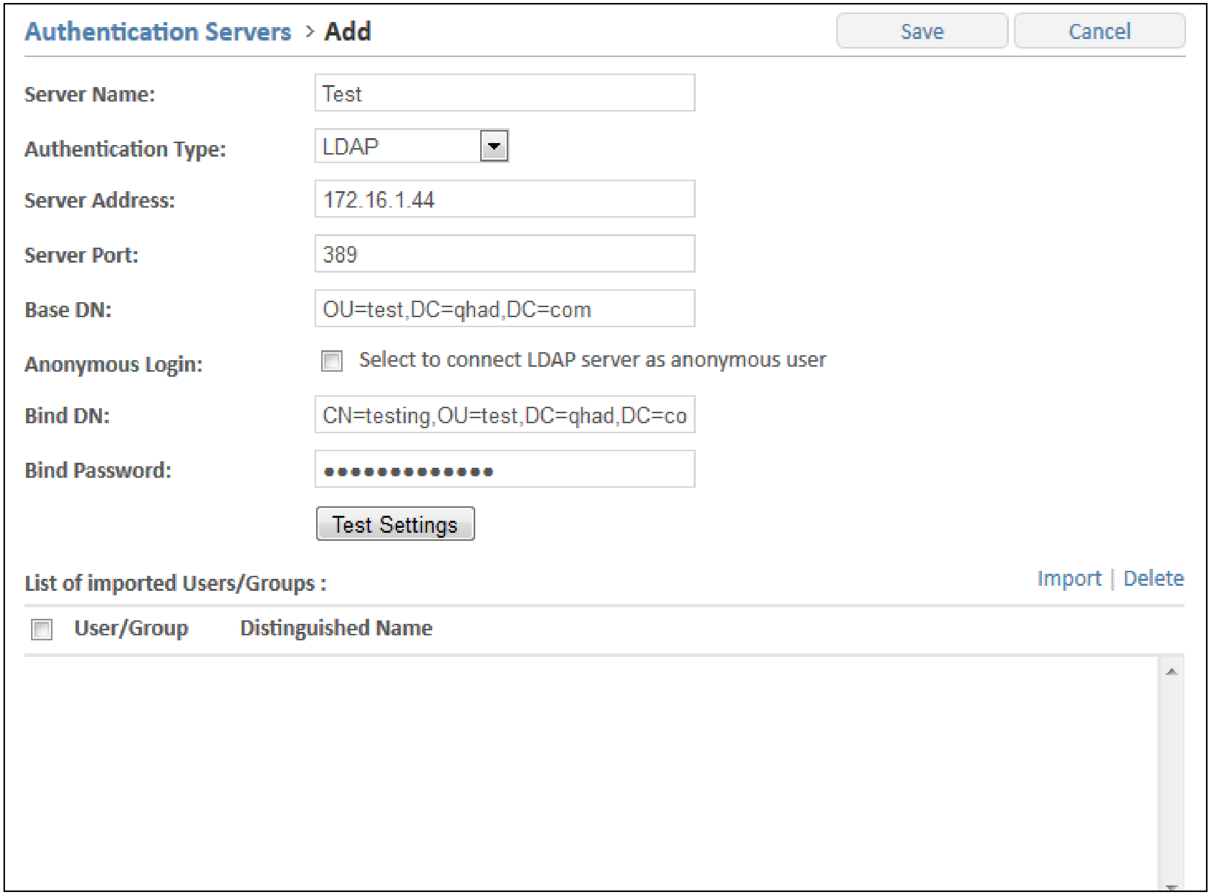


Authentication Servers

Servers

□	Name	IP Address	Port	Type	Base DN	Status
□	server1	14.141.16.16	389	LDAP	OU=test, DC=qhad,...	ON

2. Click **Add** the server details form is displayed.



Authentication Servers > Add

Server Name: Test

Authentication Type: LDAP

Server Address: 172.16.1.44

Server Port: 389

Base DN: OU=test,DC=qhad,DC=com

Anonymous Login: □ Select to connect LDAP server as anonymous user

Bind DN: CN=testing,OU=test,DC=qhad,DC=co

Bind Password: •••••••••••••

List of imported Users/Groups :

□	User/Group	Distinguished Name

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	Use this to specify the IP address of the new authentication

Field	Description
	server.
Port	Use this to specify the port number for accessing the server.
Base DN	Use this to specify 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	Use this to specify 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	Use this to specify the Bind Password that the Terminator will use for synchronizing with the Authentication servers.

4. Click **Test Settings** after you have entered all the details. The Terminator 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.

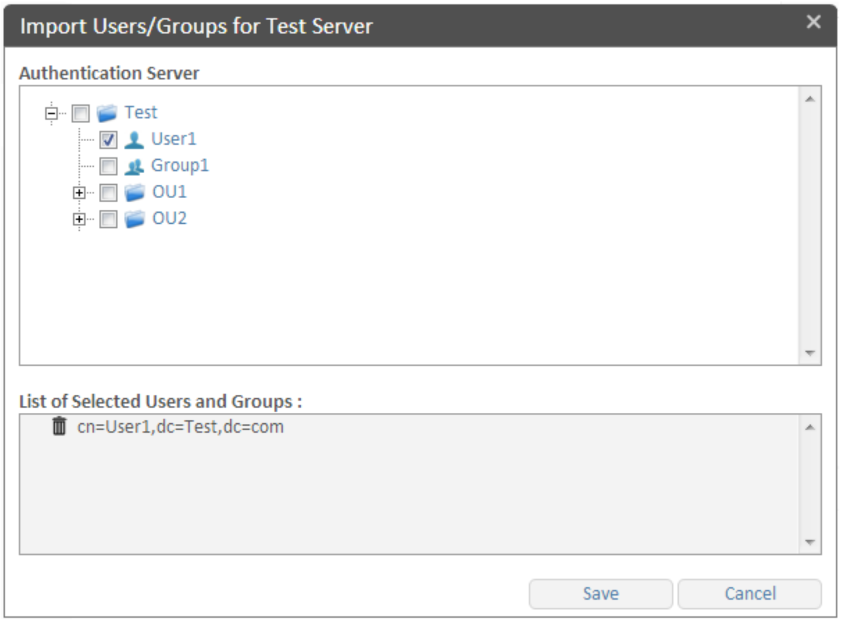
5. Click **Save**.

   All the authentication servers added are displayed in the Authentication Servers list. A summary of Name, 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. Log on to Seqrite Terminator **> 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. 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**. Terminator then connects to the configured authentication server and displays a list of the users and groups.



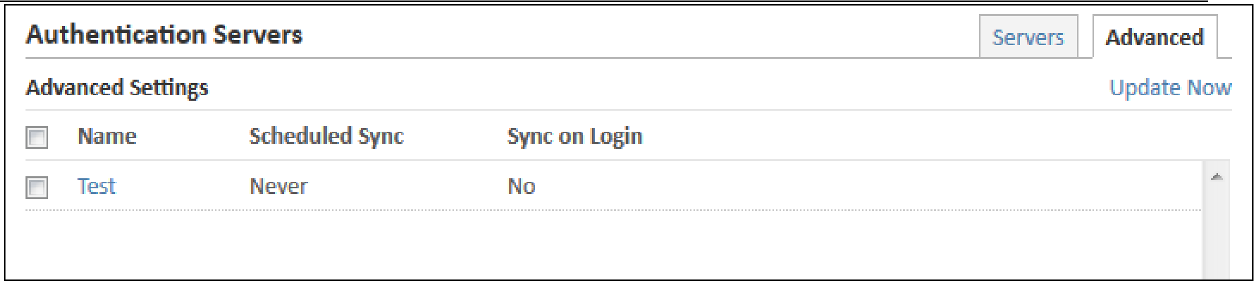
5. Carry out the following action as required:
   i. To import groups into the Terminator, select the groups and click **Import**. Details of the groups along with the users are imported into Terminator.
   ii. To delete the groups, select groups and click **Delete**. The selected groups are deleted from Terminator.

Delete Authentication servers

1. Log on to Seqrite Terminator> **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 **Delete**. You get a confirmation prompt before the Terminator 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 Terminator with the Authentication servers

1. Log on to Seqrite Terminator> **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 **Advanced**.



Authentication Servers

Advanced Settings

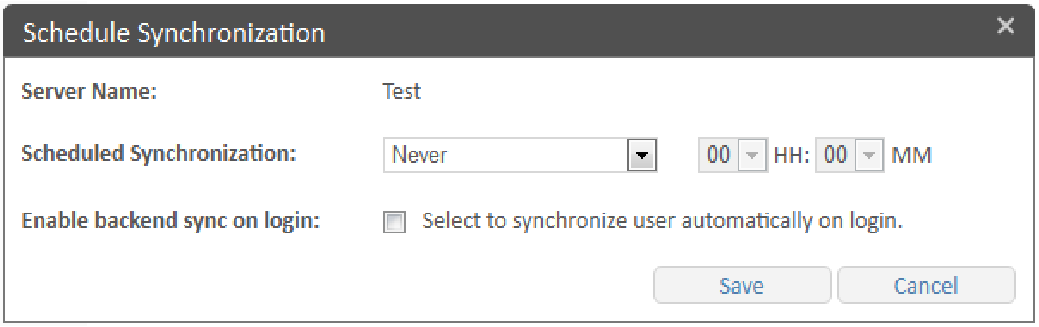
□	Name	Scheduled Sync	Sync on Login
□	Test	Never	No

3. Select a server that you want to synchronize with the Terminator and click **Update Now**. The Terminator user list is synchronized with the server user list.

Scheduling synchronization of Seqrite Terminator with Authentication servers

To schedule the synchronization of authentication server follow the steps given below:

1. Log on to Seqrite Terminator> **User Management > Authentication Servers**> **Advanced**.
2. Click on the **Server name**. The Schedule Synchronization dialog box is displayed.



Schedule Synchronization

Server Name: Test

Scheduled Synchronization: Never 00 HH: 00 MM

Enable backend sync on login: □ Select to synchronize user automatically on login.

3. From the **Schedule Synchronization** drop down list, select the frequency of synchronization as required. Select the time of synchronization in hours and minutes as required from the corresponding drop-down lists.
4. To enable synchronization automatically on login, select the option **Enable backend sync on login**.
5. Click **Save**. The Terminator user list will be synchronized with the server user list at the configured time.

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.

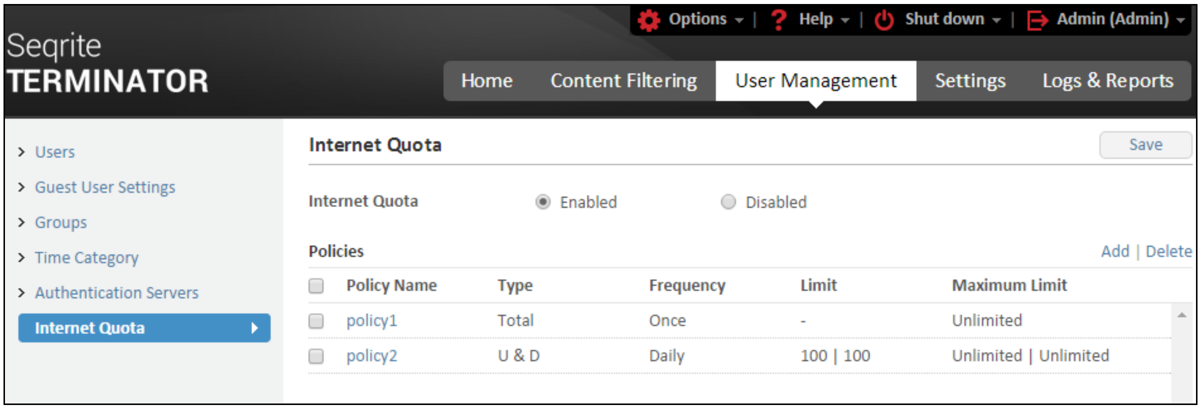
Using the Internet Quota page you can create predefined Internet Quota policy. These policies will be applied to Groups / users. If the group / user reaches the assigned quota, the Internet access will be blocked.

To configure quota management policies:

1. Log on to Seqrite Terminator **> User Management > Internet Quota**. The Internet Quota page is displayed with list of Internet Quota policies.
2. Select internet Quota as **Enabled**.

   Note:

   - Enabling Internet Quota may affect your network throughput.
   - Disabling Internet Quota will not generate bandwidth usage report.



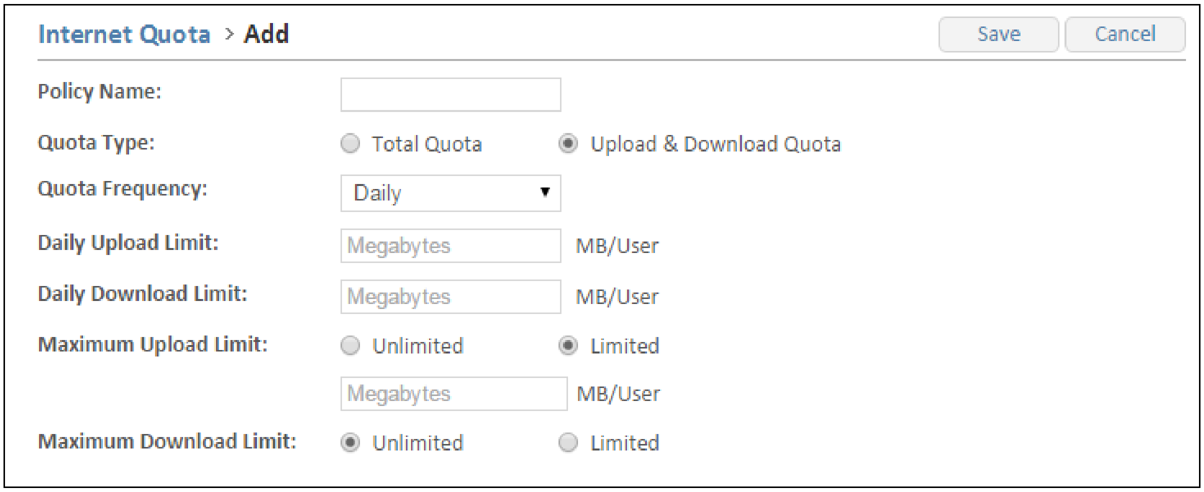
Internet Quota

Internet Quota ● Enabled ○ Disabled

Policies

□	Policy Name	Type	Frequency	Limit	Maximum Limit
□	policy1	Total	Once	-	Unlimited
□	policy2	U & D	Daily	100 | 100	Unlimited | Unlimited

3. Click **Add**, the Add internet Quota page is displayed.



Internet Quota > Add

Policy Name:

Quota Type: ○ Total Quota ● Upload & Download Quota

Quota Frequency: Daily ▾

Daily Upload Limit: Megabytes MB/User

Daily Download Limit: Megabytes MB/User

Maximum Upload Limit: ○ Unlimited ● Limited

Megabytes MB/User

Maximum Download Limit: ● Unlimited ○ Limited

The following table explains the fields on page:

Field	Description
Quota Type	You can create policy based on the total quota (upload + download) or on individual Upload & download quota. **Total Quota** then the total amount of data will be allowed, irrespective of upload and download ratio. For example, if total quota allowed is 100MB, user can use it for upload and download in any ratio.

Field	Description
	Upload & download quota the user will be restricted for fixed amount of upload and download. For example, 50MB upload and 50 MB download. If user exhausts either upload or download usage, then both upload and download will be stopped. Following table explains the field on page. If you select the **Upload and Download Quota** option, then you need to specify the individual upload and download data limit for the selected quota frequency.
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: You can set one time internet access limit which allows the user to consume the set amount of data irrespective of the period. For e.g. If 1000MB data usage is allowed for the user, then this can be consumed within day(s)/ month(s) / year(s). Daily: You can set a Daily Internet access limit. Weekly: You can set the weekly Internet access limit. If you select this option, you need to specify the day on which the week starts and the weekly data limit in MB. Monthly: You can set the Monthly internet access limit. If you select this option, you need to specify the date when you want the month to start and the monthly data limit in MB. Yearly: You can set the yearly internet access limit. If you select this option, you need to select the month from which your yearly limit should start and the yearly data limit in MB. Note: Incase there is unused data for a period, then that data 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 100MB of data usage for that day and so on. Same is applicable for other frequencies, except for “Once”.
Maximum Data limit	This is the maximum amount of data allowed for the policy. You can select the Unlimited option, which means there would be no limit on the maximum data usage. If you want the Internet access to be limited by a fixed amount of data, then select the **Limited** option and specify the

Field	Description
	maximum limit in MB.
Maximum Upload data limit	This field is displayed if you select the Quota type as Upload &Download quota. This is the maximum amount of upload data allowed for the policy. You can select the Unlimited option, which means there would be no limit on the maximum upload data usage. You can also specify a limited fixed amount of Upload data by select the **Limited** option and entering the limit in the text box.
Maximum download data limit	This field is displayed if you select the Quota type as Upload &Download quota. This is the maximum amount of download data allowed for the policy. You can select the **Unlimited** option, which means there would be no limit on the maximum download data usage. You can also specify a limited fixed amount of Download data by selecting the **Limited** option and entering the limit in the text box.

4. Click **Save**.

Chapter

7

Content Filtering & Protection

You can filter out all the content that you do not want the users on your network to access. By filtering content, you protect your network from incoming security threats and data leakage, whether done innocently or maliciously.

The protection feature helps to blocks web threats, stop malware, viruses, and phishing attacks. You can also create and enforce acceptable web usage policies.

Following Seqrite Terminator features help in content filtering and protection:

- 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.
- URL Filtering: Helps in denying access to specific Web sites from a particular domain or URL, checks all incoming and outgoing data for security policies.
- MIME Filtering: Helps to block incoming content depending on the configurations that you have set.
- Application Control: Helps in restricting insecure and low productivity applications
- Intrusion Prevention System: Helps to protect your organization's network from external application level attacks, intrusion attempts, malwares and threats

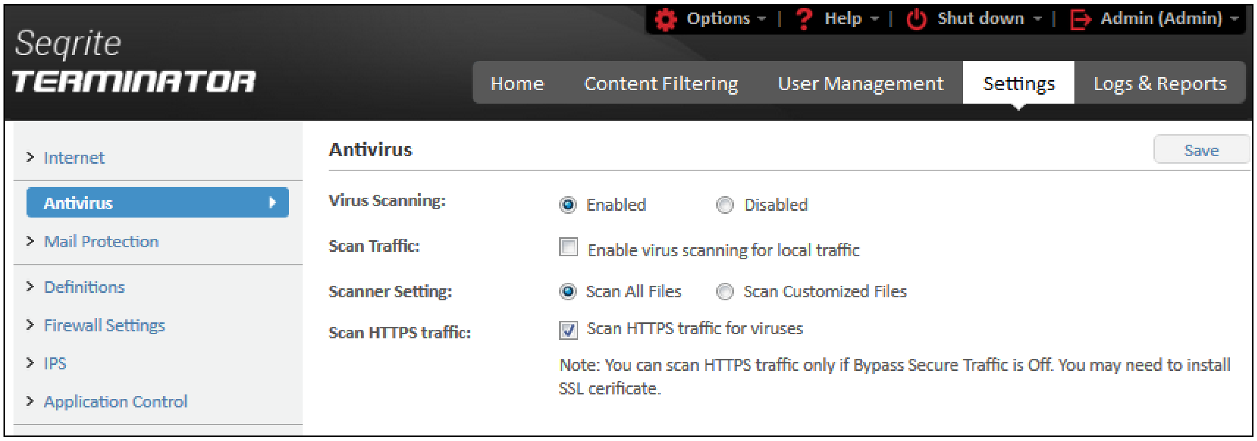
The Content filtering settings are global and are applicable to all the Users and Groups.

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 Terminator should scan. You can configure Terminator to report suspicious files and related statistics.

1. Log on to Seqrite Terminator**> Settings > Antivirus**.



Antivirus

Virus Scanning: ● Enabled ○ Disabled

Scan Traffic: □ Enable virus scanning for local traffic

Scanner Setting: ● Scan All Files ○ Scan Customized Files

Scan HTTPS traffic: ☑ Scan HTTPS traffic for viruses

Note: You can scan HTTPS traffic only if Bypass Secure Traffic is Off. You may need to install SSL cerificate.

2. Select **Enable** option to scan virus in your network.
3. Select the **Scan Traffic** option if you want to enable virus scanning for Local network.
4. The **Scanner Settings** option can be used 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.
5. You can also select to scan HTTPS traffic.

   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. (See **Internet Settings** for more details)
6. Click **Save**.

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 helps 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.

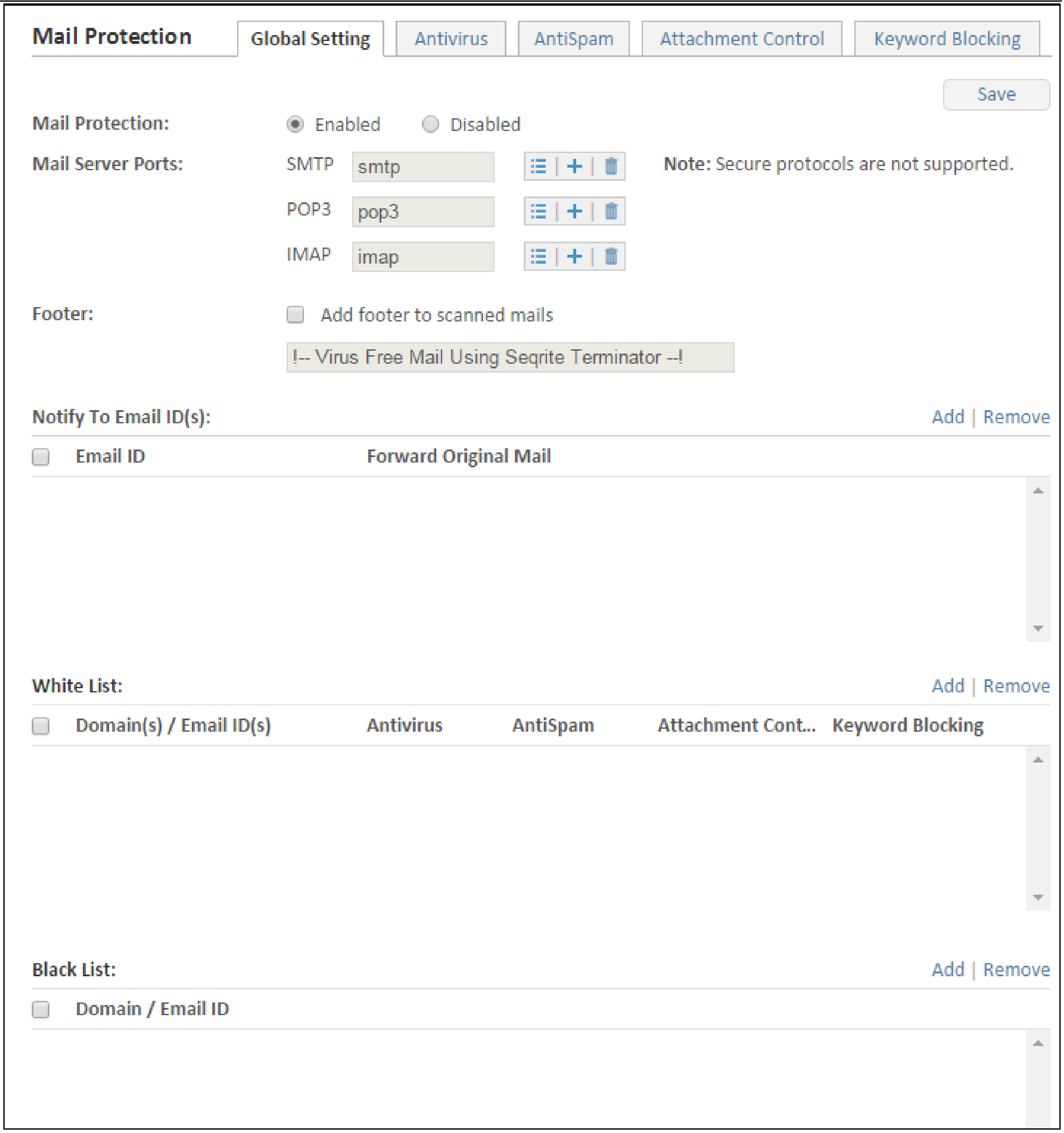
Global Settings

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

- Configure the mail server port, as the listening port of mail server SMTP, POP3, and IMAP.
- Select to add footer to the scanned emails
- Add the email ids 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.

To configure the mail protection global settings follow these steps:

1. Log on to Seqrite Terminator **> Settings > Mail Protection**. The following page is displayed.



Mail Protection: ● Enabled ○ Disabled

Mail Server Ports:

SMTP	smtp
POP3	pop3
IMAP	imap

Note: Secure protocols are not supported.

Footer: □ Add footer to scanned mails

!-- Virus Free Mail Using Seqrite Terminator --!

Notify To Email ID(s):

□	Email ID	Forward Original Mail

White List:

□	Domain(s) / Email ID(s)	Antivirus	AntiSpam	Attachment Cont...	Keyword Blocking

Black List:

□	Domain / Email ID

2. Select the **Mail Protection** option as Enabled.

3. Enter the mail server port, for SMTP, POP3 and IMAP.

4. Select the **Footer** option if you want to append a footer message in all incoming and outgoing email message. Enter the message 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.

5. 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** in the **Notify to email IDs** section. Select the option to forward the original email (that may be suspicious or infected). Click **Save**.

Note: To receive an e-mail notification, you need to configure SMTP settings first.

6. To add email address to whitelist click **Add** 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. Click **Save**.

   Note: The Email address configured in SMTP settings is by default whitelisted.

7. To add Domain / email address to blacklist click **Add** in the blacklist section. Enter Email ID / Domain name and click **Save**.

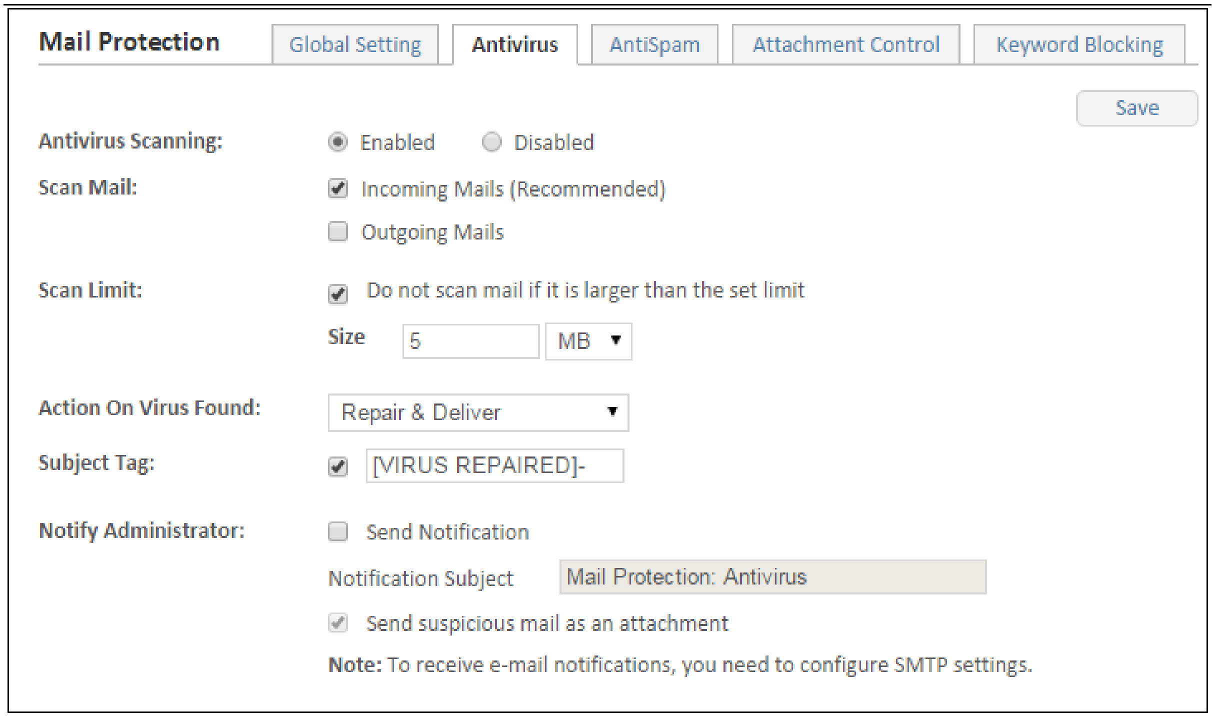
8. Click **Save** on the top right side of the Global settings page to save the Global setting configurations.

Antivirus

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 Terminator to notify the administrator in case a virus is detected and take an action on the infected mail.

To configure the Antivirus settings for mail protection follow these steps:

1. Log on to Seqrite Terminator> **Settings** >**Mail Protection >Antivirus.** The following page is displayed.



Antivirus Scanning: ● Enabled ○ Disabled

Scan Mail: ☑ Incoming Mails (Recommended)

☐ Outgoing Mails

Scan Limit: ☑ Do not scan mail if it is larger than the set limit

Size 5 MB

Action On Virus Found: Repair & Deliver

Subject Tag: ☑ [VIRUS REPAIRED]-

Notify Administrator: ☐ Send Notification

Notification Subject Mail Protection: Antivirus

☑ Send suspicious mail as an attachment

Note: To receive e-mail notifications, you need to configure SMTP settings.

2. Select Antivirus scanning option as **Enabled**.
3. Select the option to scan incoming or outgoing mail. By default incoming mails are selected for scanning.
4. Set the **Scan Limit** if you want to limit the size for emails, and 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:
   - 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.
   - 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. Select the **Notify Administrator** option to send a notification to the Admin about the infected emails. Enter the subject tag for the notification email. You can also select the option to attach the infected / suspected email and send it to the admin.
8. Click **Save**.

AntiSpam

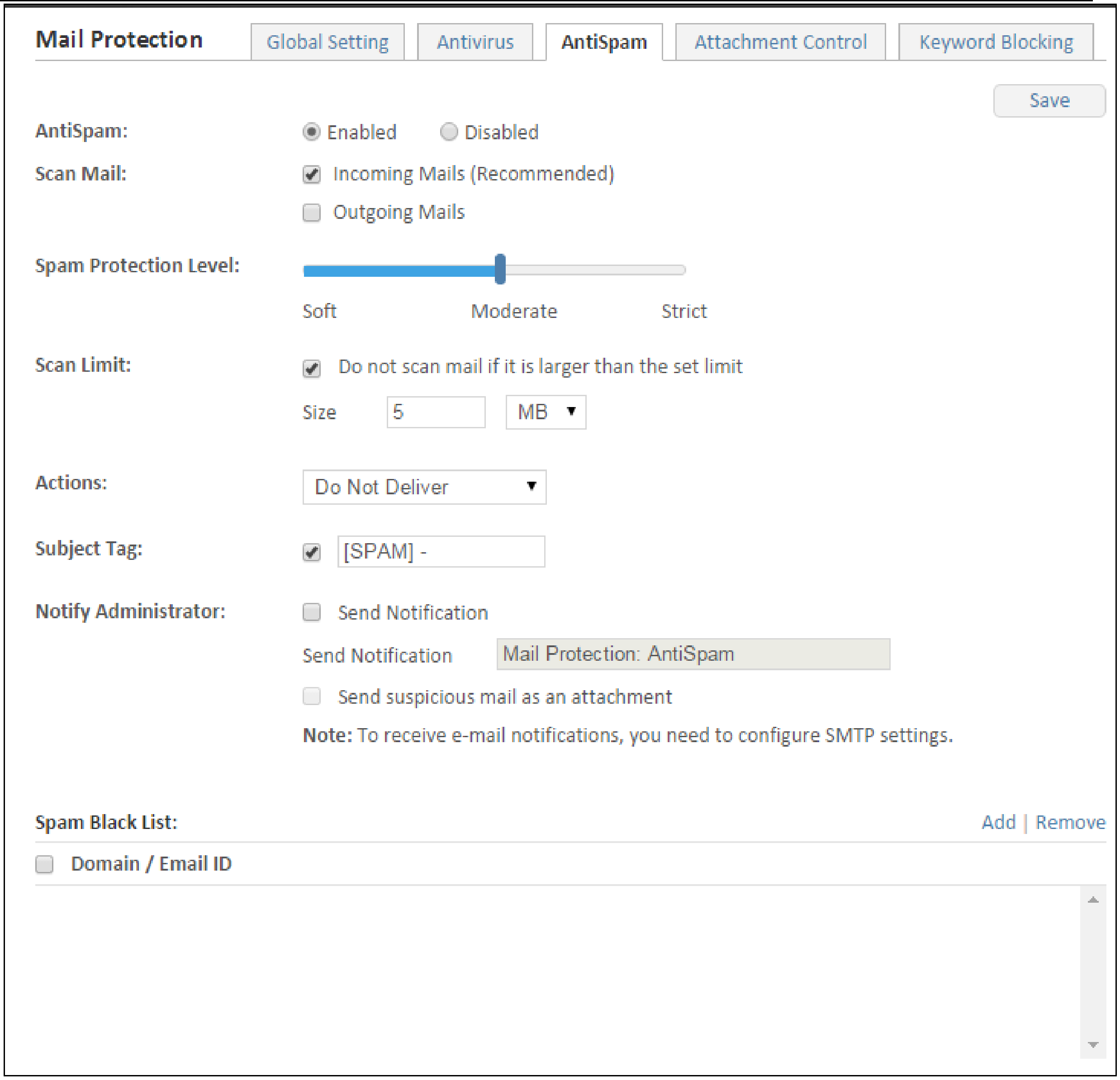
Email spam also known as unsolicited bulk E-mail (UBE), junk mail, or unsolicited commercial e-mail (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. An anti-spam feature helps to prevent email spam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

The Seqrite Terminator 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.

Note: This feature is paid and optional. You need to contact customer care to enable Anti-spam feature in your Terminator.

To configure AntiSpam settings follow the steps given below:

1. Log on to Seqrite Terminator**> Settings > Mail Protection> AntiSpam**. Following screen is displayed.



AntiSpam: ● Enabled ○ Disabled

Scan Mail: ☑ Incoming Mails (Recommended)

☐ Outgoing Mails

Spam Protection Level: Soft Moderate Strict

Scan Limit: ☑ Do not scan mail if it is larger than the set limit

Size 5 MB

Actions: Do Not Deliver

Subject Tag: ☑ [SPAM] -

Notify Administrator: ☐ Send Notification

Send Notification Mail Protection: AntiSpam

☐ Send suspicious mail as an attachment

Note: To receive e-mail notifications, you need to configure SMTP settings.

Spam Black List:

☐ Domain / Email ID

2. Select Antispam as **Enabled** to scan all the incoming mails for spam.
3. Select **Scan Mail** option. You can set whether to scan only incoming mails or both incoming and outgoing mails for spam.
4. Set a **Spam protection Level**. 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 **Scan 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 **Notify Administrator** option to send a notification to the Admin 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.

9. You can 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.

   To enter Email IDs to Spam blacklist click **Add** in the Spam blacklist section. Enter the Email ID in the given textbox and click **Save**.

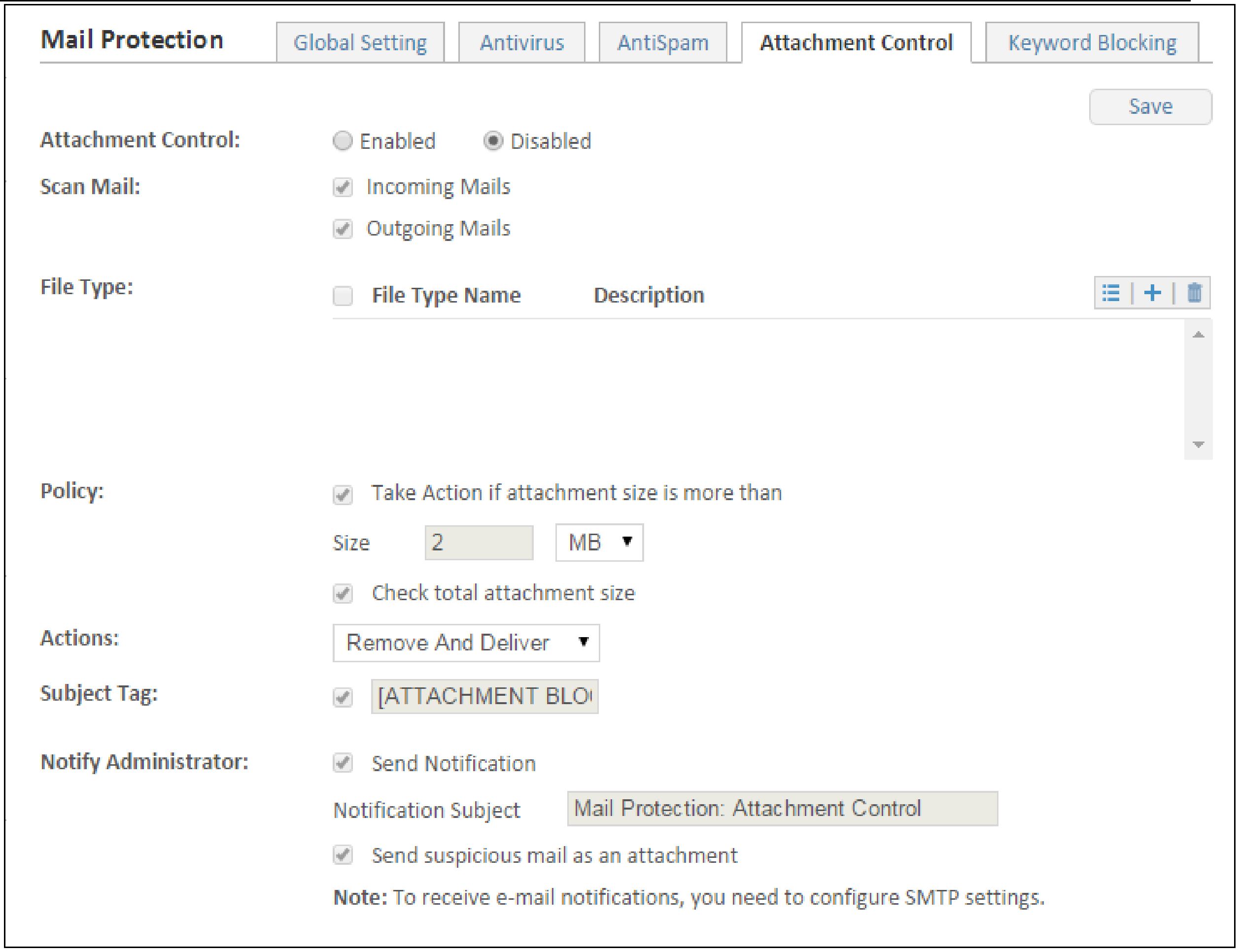
10. To save the configurations of the Antispam page click **Save** on the right hand side of the page**.**

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.

To configure attachment control follow these steps:

1. Log on to Seqrite Terminator**> Settings > Mail Protection > Attachment Control**. Following screen is displayed.



Attachment Control: ○ Enabled ● Disabled

Scan Mail: ☑ Incoming Mails

☑ Outgoing Mails

File Type: □ File Type Name Description

Policy: ☑ Take Action if attachment size is more than

Size 2 MB

☑ Check total attachment size

Actions: Remove And Deliver

Subject Tag: ☑ [ATTACHMENT BLO

Notify Administrator: ☑ Send Notification

Notification Subject Mail Protection: Attachment Control

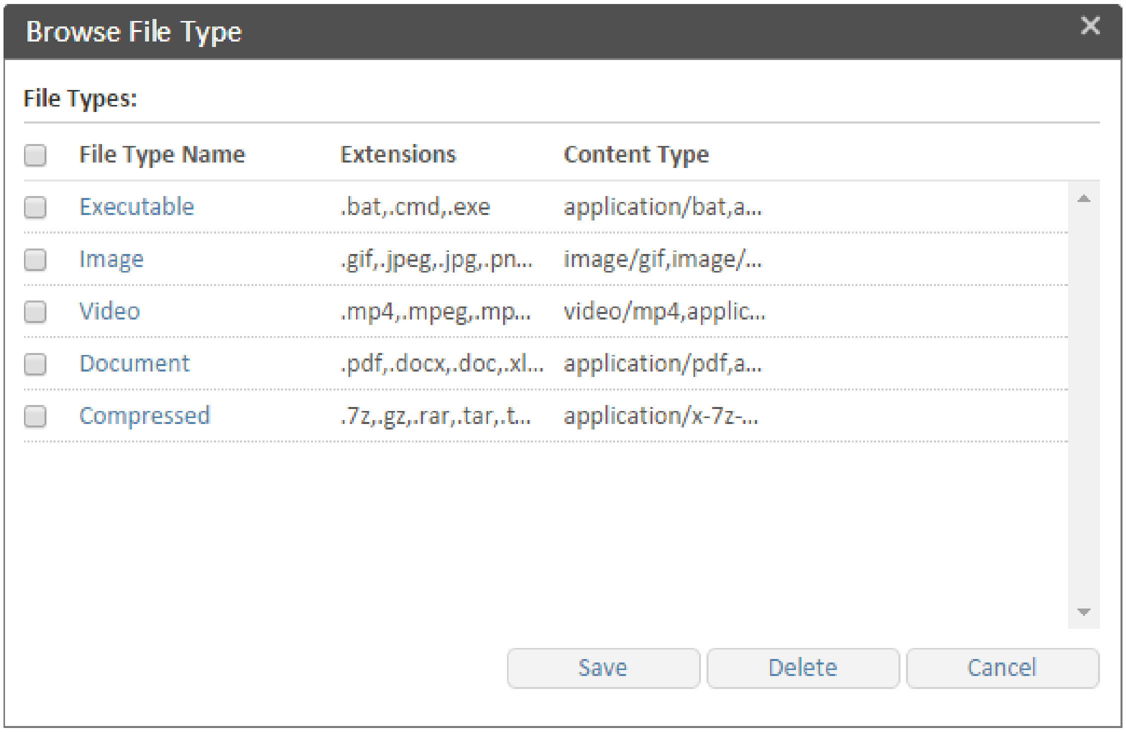
☑ Send suspicious mail as an attachment

Note: To receive e-mail notifications, you need to configure SMTP settings.

2. Select Attachment control as **Enabled**.
3. Select **Scan Mail** option. You can set whether to scan only incoming mails or both incoming and outgoing mails for attachment control.
4. Select the option in 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 the **File type**. You can add, browse and delete 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.



Browse File Type

File Types:

□	File Type Name	Extensions	Content Type
□	Executable	.bat,.cmd,.exe	application/bat,a...
□	Image	.gif,.jpeg,.jpg,.pn...	image/gif,image/...
□	Video	.mp4,.mpeg,.mp...	video/mp4,applic...
□	Document	.pdf,.docx,.doc,.xl...	application/pdf,a...
□	Compressed	.7z,.gz,.rar,.tar,.t...	application/x-7z-...

6. Select **Action** to be taken on the spam email from the following two actions:
   - Send original: Sends the original email
   - Do not deliver: In case of SMTP email will be blocked and in case of POP3 original mail without attachment will be sent.
   - Remove and Deliver: Removes the attachment and sends the email.
7. Select the **Subject Tag** option if you want to prefix to the email subject for the attachment control scanned email. Enter the Subject Tag in the given textbox.
8. Select the **Notify Administrator** option to send a notification to the Admin about the malicious attachment in the 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.
9. Click **Save** on the right hand side of the Attachment control page to save the configurations.

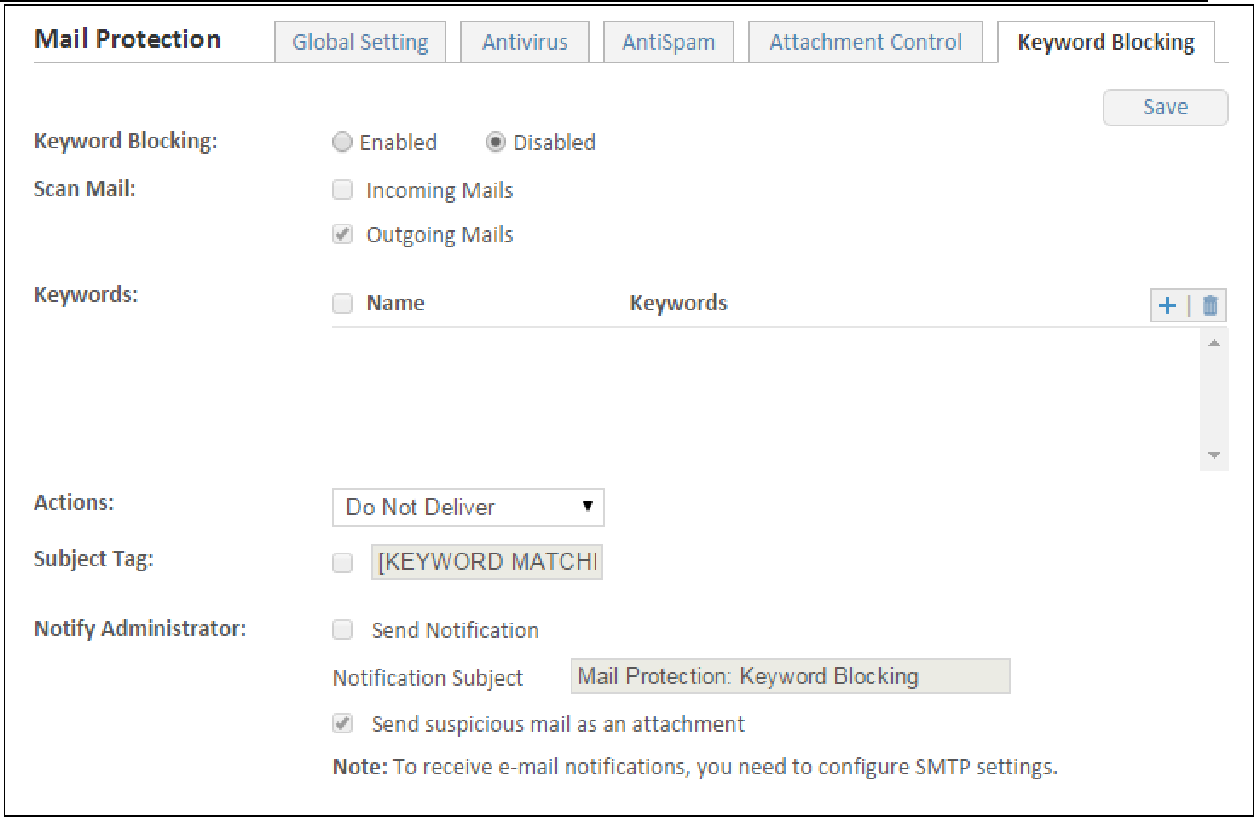
Keyword Blocking

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.

To configure keyword blocking, follow these steps:

1. Log in to Seqrite Terminator**> Settings> Mail Protection> Keyword Blocking**. The Keyword blocking page is displayed.



Keyword Blocking: ○ Enabled ● Disabled

Scan Mail: □ Incoming Mails ☑ Outgoing Mails

Keywords:

□	Name	Keywords

Actions: Do Not Deliver ▾

Subject Tag: □ [KEYWORD MATCHI

Notify Administrator: □ Send Notification

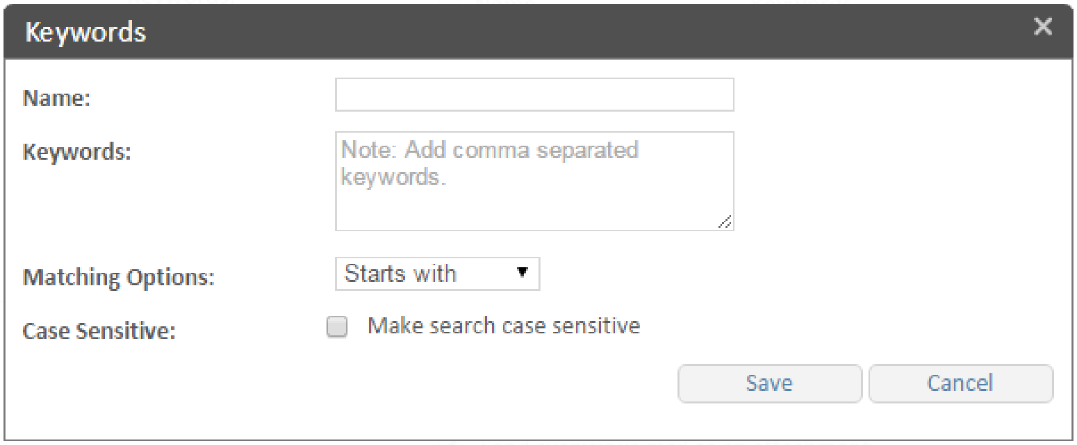
Notification Subject: Mail Protection: Keyword Blocking

☑ Send suspicious mail as an attachment

Note: To receive e-mail notifications, you need to configure SMTP settings.

2. Select **Keyword Blocking** as Enabled.

3. Select the keyword that you want to search in the subject / body of the email. You can also add new keyword using the plus (+) icon provided. On clicking this icon the Add keyword popup is displayed. The following table explains the fields in the popup.



Name:

Keywords: Note: Add comma separated keywords.

Matching Options: Starts with ▾

Case Sensitive: □ Make search case sensitive

Field	Description
Name	Enter a name for the keyword. This name will be used for identification.
Keyword	Enter the keywords.
Matching Option	**Starts with**: Searches the email for the words that start with the mentioned keyword. For e.g. If you add “son” as the keyword, then email with words like son, sony, sonic, will be blocked, whereas emails with words like person, peterson will not be blocked. **Ends with**: Searches the email for the words that ends with the mentioned keyword. For e.g. If you add “son” as the keyword, then emails containing the words like sony, sonic, will not be blocked. However email containing words like son, person, peterson will be blocked. **Exact Match**: Searches the email for the entire keyword. If the email contains the words that match exactly as the specified keyword, the email will be blocked. **In Between**: Searches the email for the sentence containing the keyword.
Case Sensitive	Select this option if you want the keyword search to be case sensitive. For e.g. If you add the keyword “Ocean” to be blocked and marked it as case sensitive then, the email containing the words OCEAN, oCean, OceAn etc will not be blocked.

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. Select the **Subject Tag** option if you want to prefix to the email subject for the attachment control scanned email. Enter the Subject Tag in the given textbox.
6. Select the **Notify Administrator** option to send a notification to the Admin about the keyword blocking email. 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.
7. Click **Save** on the right hand side of the Keyword Blocking page to save the configurations**.**

URL Filtering

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 Content Filtering Web sites are grouped under allowed and denied categories. You can move Web sites under these categories based on the content, e.g. Advertisement, Jobs, Downloads, etc. can be moved under denied categories.

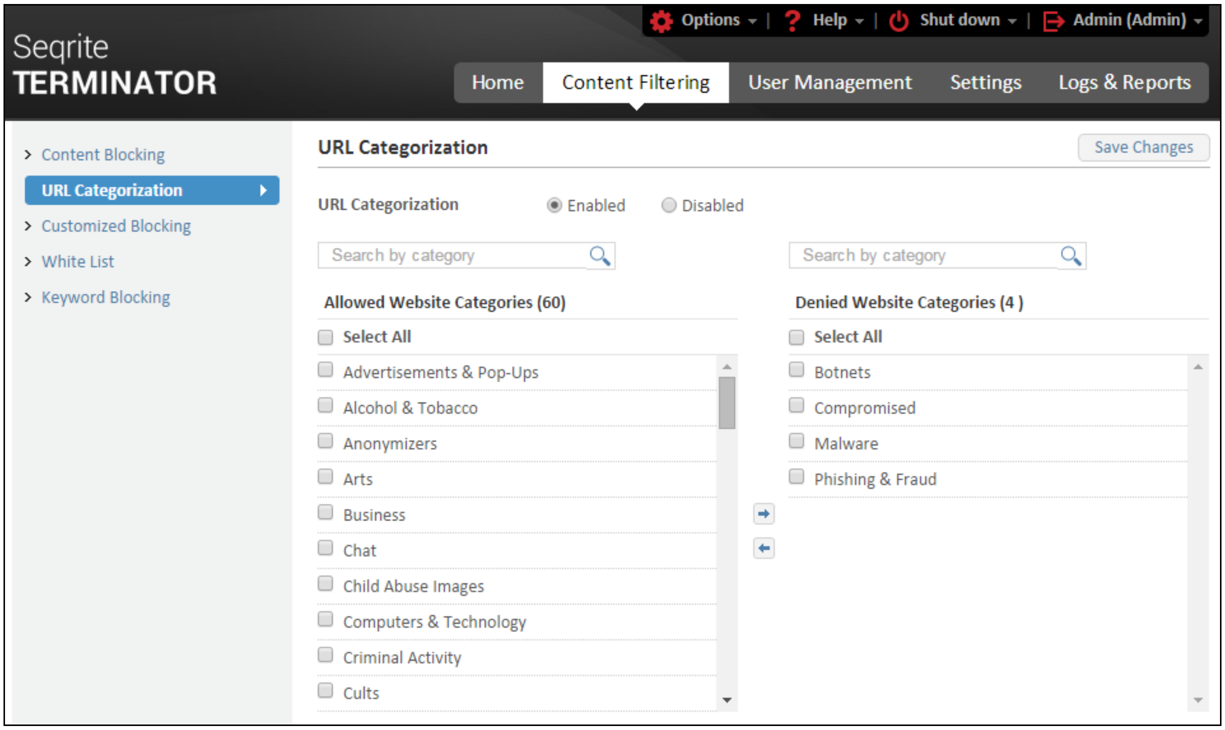
Category Based Web site blocking (URL Categorization)

Category based blocking is Web site blocking based on a category to which a Web site or pages may belong. When accessing the blocked pages or Web site a message is displayed indicating that the page was blocked as per the blocking policy. An entry is also made in the Policy Breach report. By default categories like Malware, Botnets, Compromised, and Phishing & Fraud are in Denied List.

Web site blocking is useful for various reasons. It is used to protect network, prevent access to inappropriate sites with offensive material or access to social networking sites, etc. Web site blocking restricts access to limited sites, which helps to increase the organizational work efficiency.

To block a Web site based on category, follow these steps:

1. Log on to Seqrite Terminator **> Content Filtering > URL Categorization**. The Website Blocking options page displays the list of allowed and denied Web site categories.



URL Categorization

URL Categorization ● Enabled ○ Disabled

Allowed Website Categories (60)

- □ Select All
- □ Advertisements & Pop-Ups
- □ Alcohol & Tobacco
- □ Anonymizers
- □ Arts
- □ Business
- □ Chat
- □ Child Abuse Images
- □ Computers & Technology
- □ Criminal Activity
- □ Cults

Denied Website Categories (4)

- □ Select All
- □ Botnets
- □ Compromised
- □ Malware
- □ Phishing & Fraud

2. Select the **URL Categorization** option as enabled.
3. Select a Web site category that you want to block. You can also enter the name in the **Search by Category** text box to search for a category.
4. Click the right arrow button to move the selected category to the **Denied Website Categories** list. To move a category to the Allowed Websites category, select the category and click the other left arrow button.
5. Click **Save Changes**.

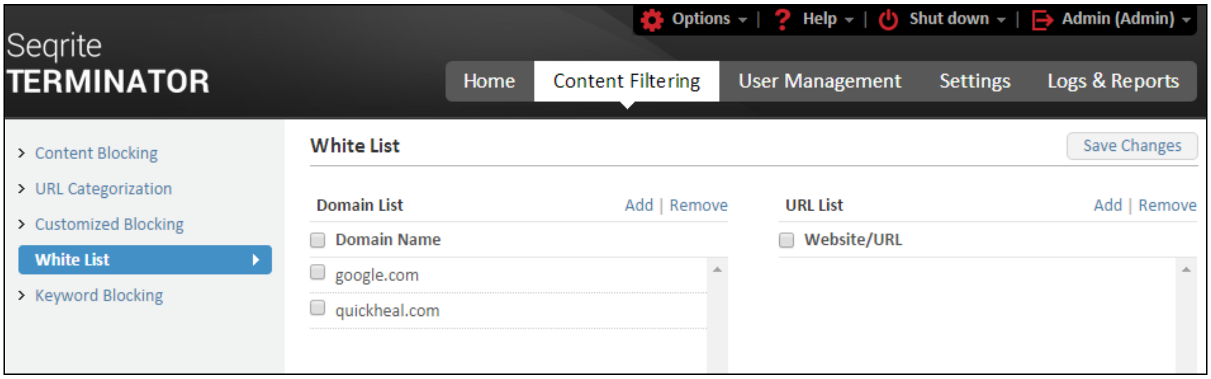
   Note: If the Device is in offline mode and Web Security service is selected to be offline then the URL categorization will not work.

White List

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.

To add Web sites to the White list follow the steps given below:

1. Log on to Seqrite Terminator **> Content Filtering > White List**. This page displays the list of the domains, Web sites and URLs that have been added to the White List.



2. Click **Add** in the Domain list / URL list, a text box is displayed. Enter in the domain name / URL / IP address that you want to add to the White list.
3. Click **Save**.
4. Click **Save changes** on the upper right side to save the changes.

Remove Web sites from the White list:

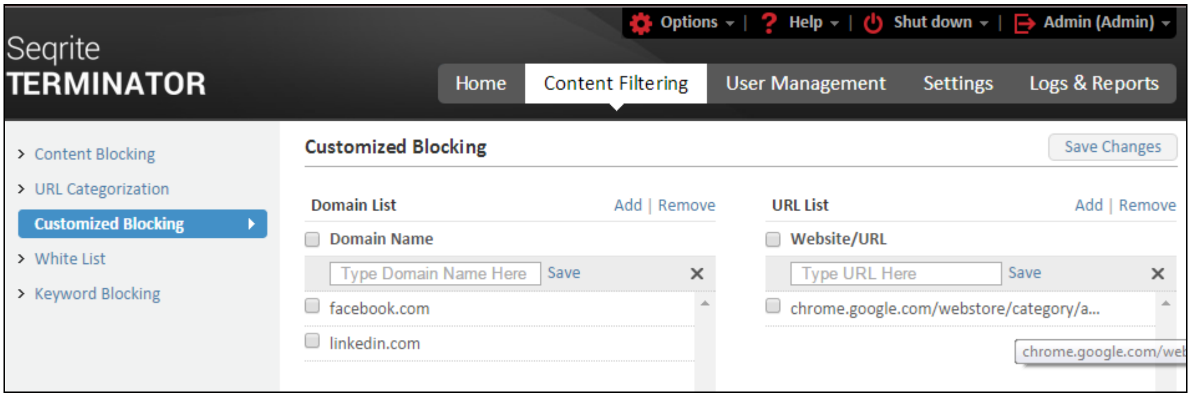
1. Log on to Seqrite Terminator**> Content Filtering > White List**. This page displays the list of the Web sites that have been added to the White List.
2. Select the domain name or Web site/URL that you want to remove from the White list and click **Remove**.
3. Click **Save changes** on the upper right side to save the changes.

Blacklist (Customized Blocking)

This feature on the Seqrite Terminator allows you to block the sites that you do not want users on your network to access. You can specify the sites that you want to block by adding either their URLS, domain names, or IP addresses.

To block Web sites URLS/Domain names follow the steps given below:

1. Log on to Seqrite Terminator **> Content Filtering > Customized Blocking**. This page displays the Domain list and the URL list of the blocked Web sites.
2. In the Domain list area, click **Add**.



3. Enter the domain Name or the IP address that you want to block in the designated text box. For e.g. google.com. If you want to block a URL or an IP address, add the URL/IP address under the Website/URL list.

   If the Web site or URL is entered with 'http://' then it will be stripped and added to the list.

4. Click **Save**. The domain name/URL is added to the list of blocked domain names.

Remove Web sites URLS/Domain names from blocked list

To remove the URLS/ domain names from blocked list follow the steps given below:

1. Log on to Seqrite Terminator> **Content Filtering**> **Customized Blocking**. The Customized Blocking options page displays the Domain list and the URL list of the blocked Web sites.
2. In the Domain list area, select the Web site/ URL that you want to remove from the blocked list and click **Remove**.
3. Click **Save Changes**. The domain name/URL is removed from the list of blocked domain names.

MIME Filtering

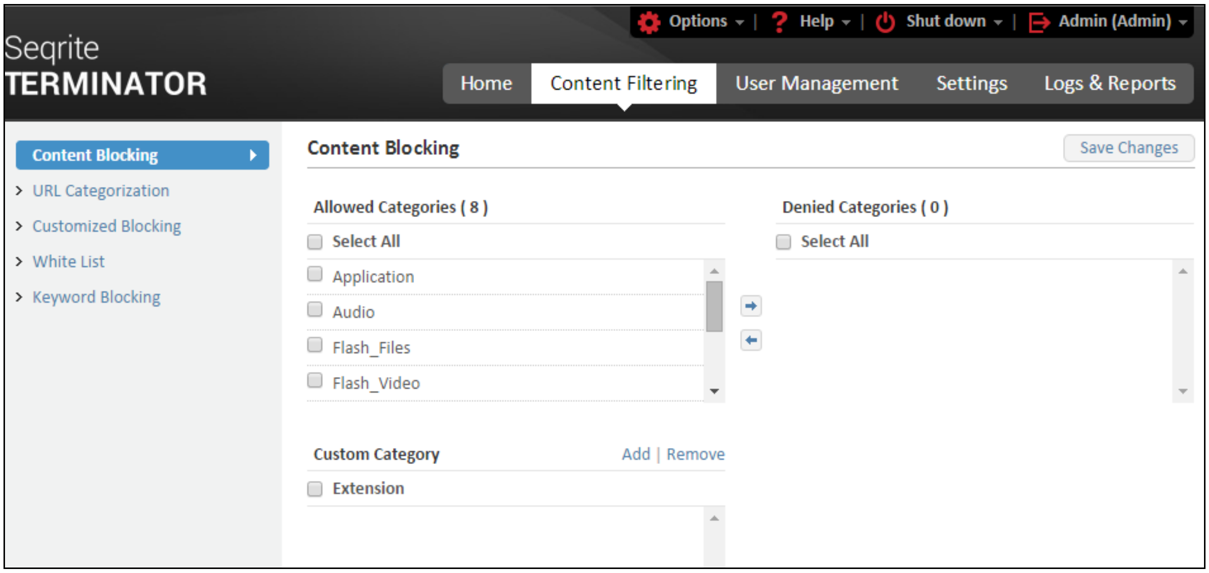
Using the Content blocking feature on the Seqrite Terminator, you can block content based on file types. You can blocks the files based on MIME types or the extensions. Some MIME types have been grouped in a category (For EG: Audio- .WMV, .WMA, .MP4, .MP3).

You can either allow or deny the specified category file types on the network. If you want to add or remove specific extensions, you can do so in the Custom Category list. Content marked under the Allowed categories is not blocked for users. However, all the Content from Denied categories and customs category is blocked to the users.

Default MIME Filtering

To block/unblock MIME types follow the steps given below:

1. Log on to Seqrite Terminator> **Content Filtering**. The Content Blocking page is displayed. This page displays the list of allowed and denied categories.



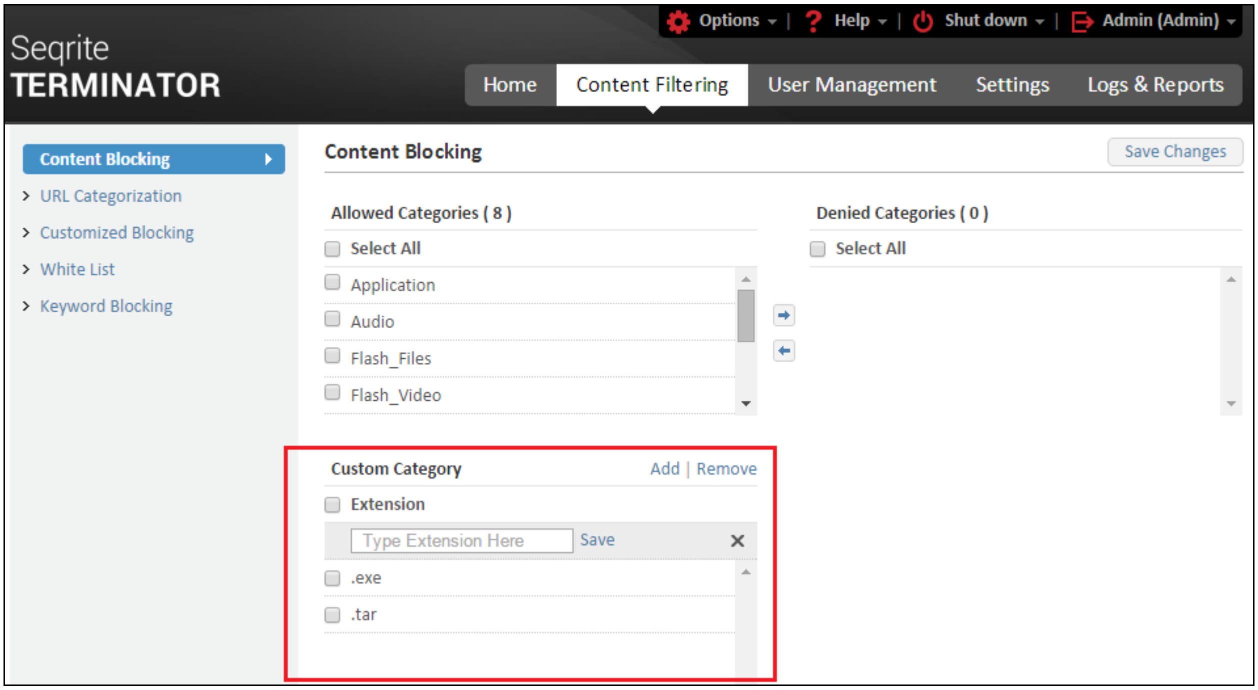
2. Select the content type from the Allowed Categories that you want to deny, click the right arrow button to move the selected content type to the Denied categories list. Similarly, to move a content category from the Denied category to the Allowed category, select the content type and click the left arrow button.
3. Click **Save Changes**.

Custom MIME Filtering

You can add the extension of the file types that need to be blocked. Enter the extension without any dot. For example, exe, tar.

To add custom file extensions for blocking follow the steps given below:

1. Log on to Seqrite Terminator> **Content Filtering**. The Content Blocking page displays the list of allowed and denied categories.



2. In the Custom Category list, click **Add** and enter the extension of the files that you want to block in the designated text box. Click **Save** to save the Custom category in the list.

3. Click **Save Changes** to save the added categories or file types.

Remove custom file extensions from being blocked

1. Log on to Seqrite Terminator> **Content Filtering**. The Content Blocking options page displays the list of allowed and denied categories.

2. In the Custom Category list, select the extension type that you want to remove from the blocked list and click **Remove**.

3. Click **Save Changes** to save changes.

Keyword Blocking

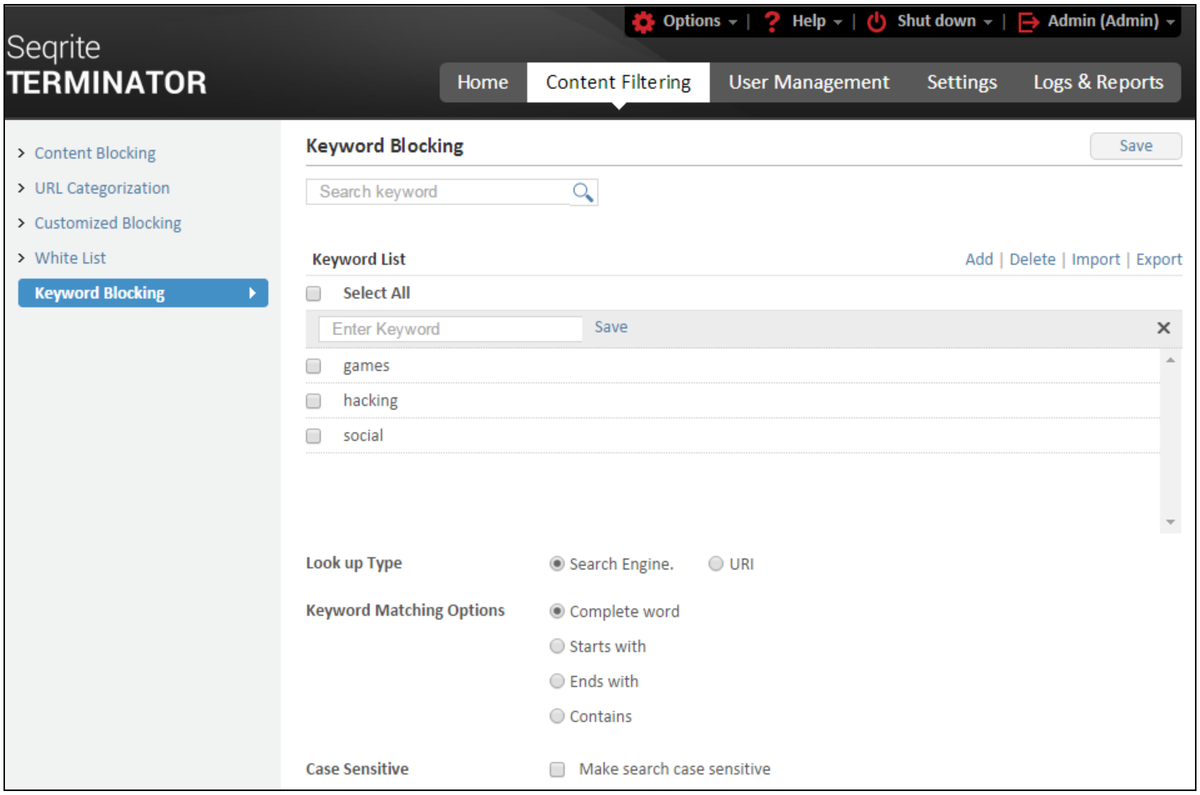
A keyword is a string of characters like a word, a number, or an acronym which can be searched through a search engine or the keyword may be present in URIs of Web sites. Seqrite Terminator provides HTTP/HTTPS content blocking based on keywords.

Using the Keyword blocking feature you can choose to block the keyword in search engines or in the URI of Web sites. For example, if you add "Hacking" to the list of keywords, it will be blocked in the search engine or the website containing the keyword “Hacking” in the URI address will be blocked.

To configure keyword blocking, follow these steps:

1. Log in to Seqrite Terminator **> Content Filtering > Keyword Blocking**. The Keyword blocking page is displayed.

2. Click **Add**. Enter the keyword in the textbox.



Keyword Blocking

Keyword List

□ Select All

Enter Keyword

□ games

□ hacking

□ social

Look up Type ● Search Engine. ○ URI

Keyword Matching Options ● Complete word ○ Starts with ○ Ends with ○ Contains

Case Sensitive □ Make search case sensitive

3. Click **Save**, the keyword will be added in the list.

   Note: You can add multiple keywords by importing a list of keywords from .csv file. You can also export the keywords in .csv file format.

4. The following table explains the fields on page:

Field	Description
Lookup Type	Select to block the keyword in search engine or URI.
Keyword Matching Option	**Complete word**: Block entire keyword in search query / Web site URI. **Starts with**: Block search query / URI for the words that start with the mentioned keyword. For e.g. If you add “son” as the keyword, words like sony, sonic, will be blocked from search and URI, whereas words like person, peterson will not be blocked. **Ends with**: Block search query / URI for the words that ends with the mentioned keyword. For e.g. If you add “son” as the keyword, words like sony, sonic, will not be blocked from search and URI. However words like person, peterson will be blocked. **Contains**: Block search / website URI containing the keyword.

Case Sensitive	Select this option if you want the keyword search to be case sensitive. For e.g. If you add the keyword “Ocean” to be blocked and marked it as case sensitive then, the words OCEAN, oCean, OceAn etc. will not be blocked.

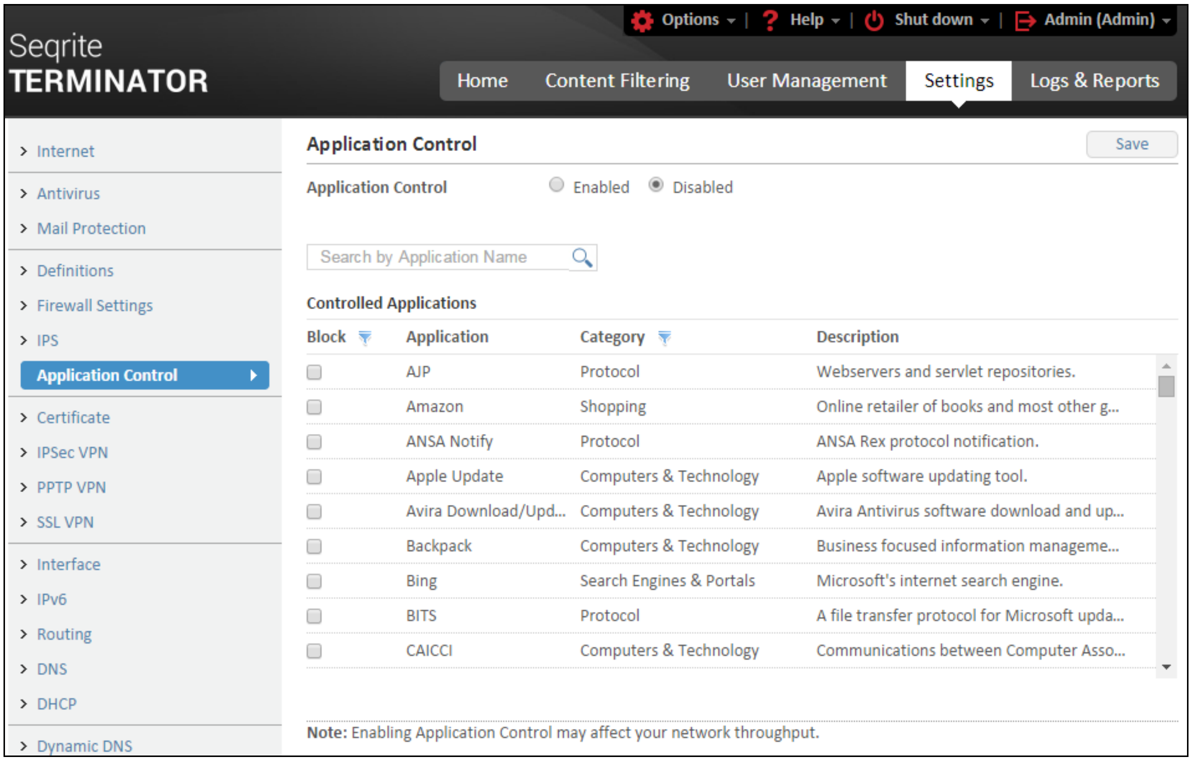
Note: To block HTTPS keywords, you need to enable “Virus scanning for HTTPS traffic”. (For more details see Antivirus.)

Application Control

Seqrite Terminator Application Control helps in restricting insecure and low productivity applications from monitored network environments thus saving on Internet bandwidth consumption. It provides a database of 800+ 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.

To enable application control follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > Application Control**. The Application Control screen is displayed.



Application Control

Application Control ○ Enabled ● Disabled

Controlled Applications

Block	Application	Category	Description
□	AJP	Protocol	Webservers and servlet repositories.
□	Amazon	Shopping	Online retailer of books and most other g...
□	ANSA Notify	Protocol	ANSA Rex protocol notification.
□	Apple Update	Computers & Technology	Apple software updating tool.
□	Avira Download/Upd...	Computers & Technology	Avira Antivirus software download and up...
□	Backpack	Computers & Technology	Business focused information manageme...
□	Bing	Search Engines & Portals	Microsoft's internet search engine.
□	BITS	Protocol	A file transfer protocol for Microsoft upda...
□	CAICCI	Computers & Technology	Communications between Computer Asso...

Note: Enabling Application Control may affect your network throughput.

2. To Enable or Disable, Application Control feature, click on Enable or Disable radio button.

3. By Default all the controlled applications are allowed. Select the Application Name you want to block.

4. Click **Save**. The selected applications will be blocked.

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 Terminator 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 Terminator either drops the packet or sets up an alarm.

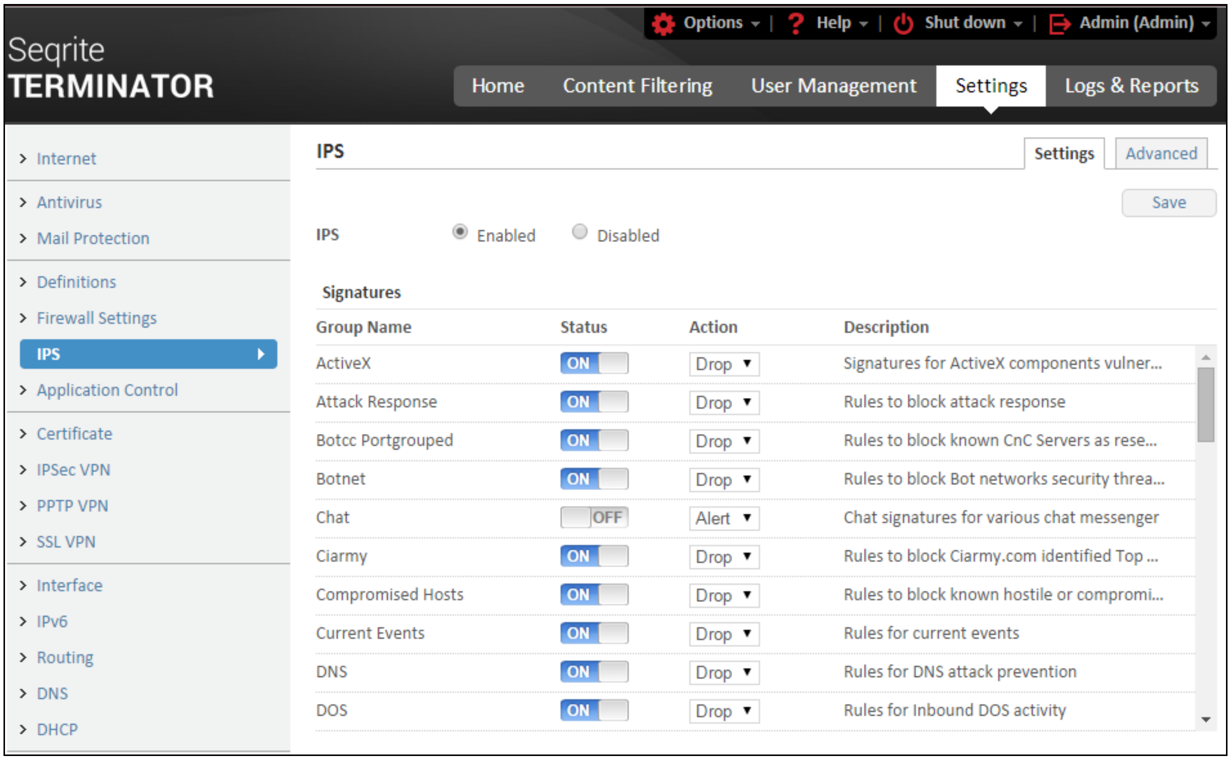
Seqrite IPS can take the following actions depending on what it has been programmed to do:

- 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.

Default Rules

To configure the IPS follow the steps given below:

1. Log on to Seqrite Terminator >**Settings > IPS**. The following page is displayed with the list of signature groups, the current status, the actions and the descriptions:



IPS

IPS ● Enabled ○ Disabled

Signatures

Group Name	Status	Action	Description
ActiveX	ON	Drop	Signatures for ActiveX components vulner...
Attack Response	ON	Drop	Rules to block attack response
Botcc Portgrouped	ON	Drop	Rules to block known CnC Servers as rese...
Botnet	ON	Drop	Rules to block Bot networks security threa...
Chat	OFF	Alert	Chat signatures for various chat messenger
Ciarmy	ON	Drop	Rules to block Ciarmy.com identified Top ...
Compromised Hosts	ON	Drop	Rules to block known hostile or compromi...
Current Events	ON	Drop	Rules for current events
DNS	ON	Drop	Rules for DNS attack prevention
DOS	ON	Drop	Rules for Inbound DOS activity

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.

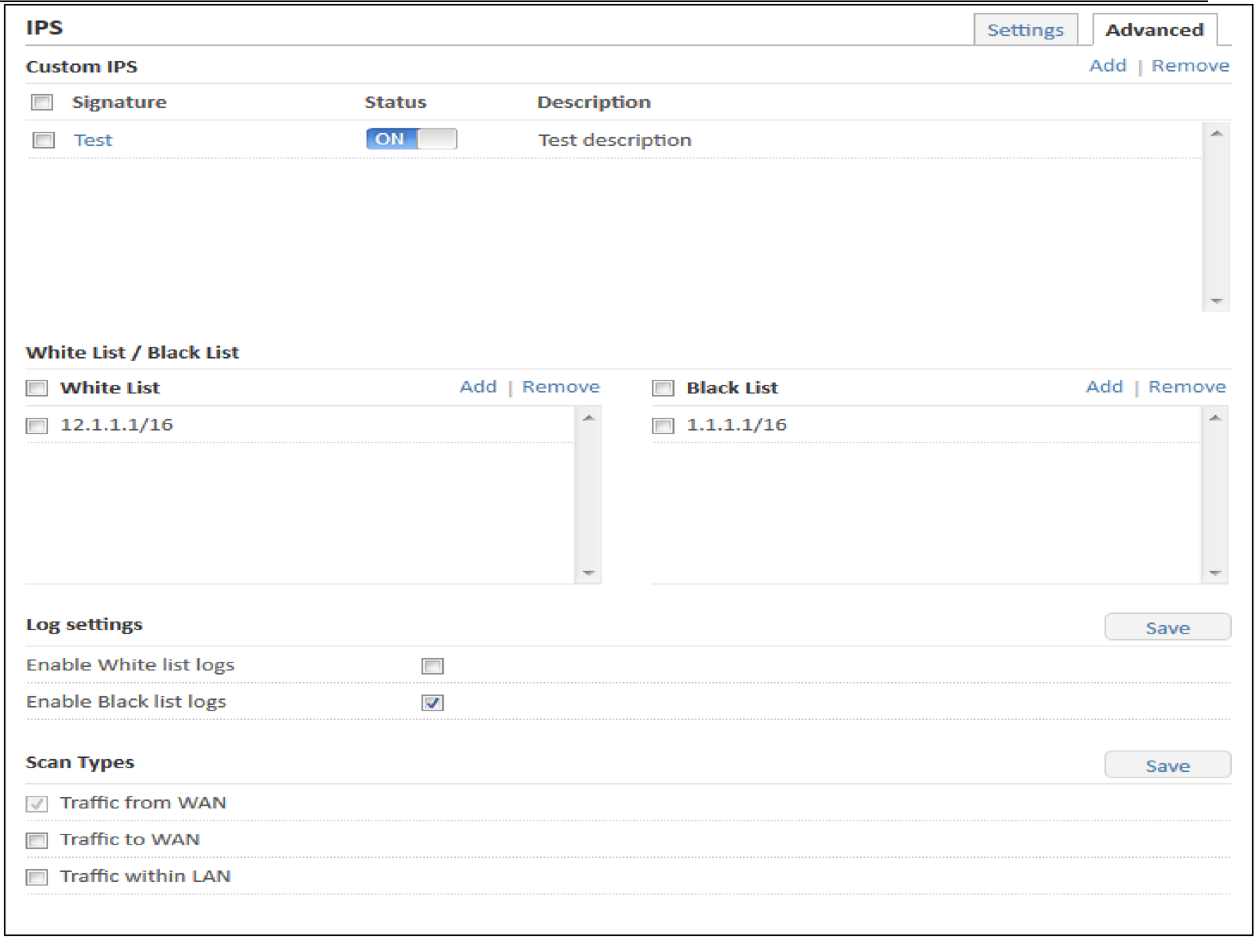
3. Click **Save**.

Custom Rules

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

To add a custom signature for intrusion prevention follow the steps given below:

1. Log on to Seqrite Terminator> **Settings** > **IPS**> **Advanced**. The Custom IPS screen is displayed.



Custom IPS

□ Signature	Status	Description
□ Test	ON	Test description

White List / Black List

□ White List	□ Black List
□ 12.1.1.1/16	□ 1.1.1.1/16

Log settings

Enable White list logs □

Enable Black list logs ☑

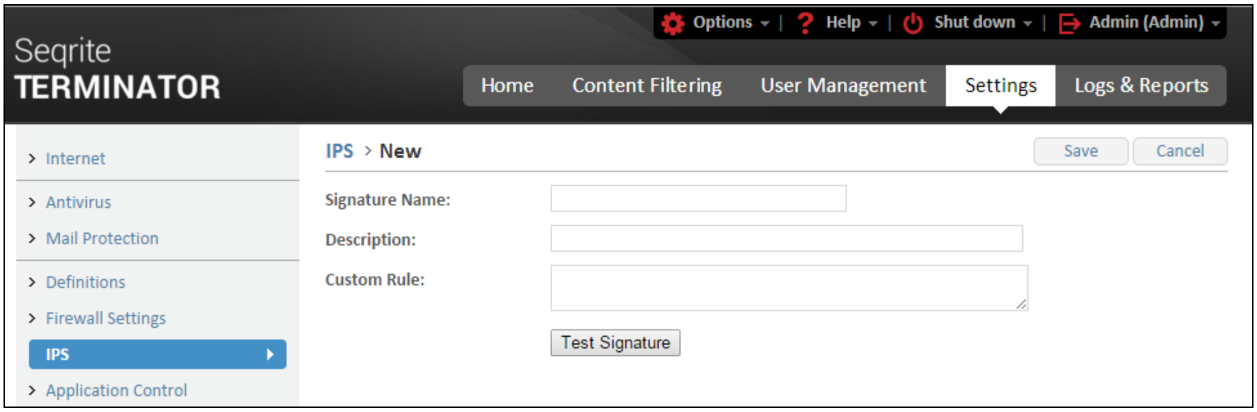
Scan Types

☑ Traffic from WAN

□ Traffic to WAN

□ Traffic within LAN

2. Click **Add**. The Custom IPS signature screen is displayed.



Signature Name:

Description:

Custom Rule:

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. Click **Test Signature** to test the signature. This will let you know if the signature is valid or not.
5. If the signature is validated, click **Save** to add it to the Terminator database.

White List / Black List

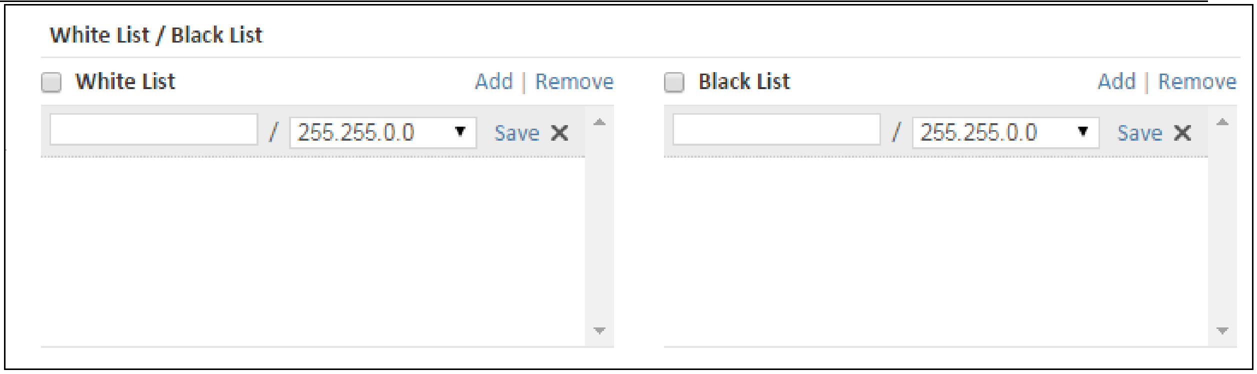
In Internet terminology, a white list is a generic name for a list of IP addresses that are considered harmless or genuine. Whitelists are used frequently in network security systems to allow users to compile lists of IP addresses they wish to receive or send packets to. The packets received from the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

Adding IP addresses to the White / Black list

To add IP address to whitelist/ blacklist follow the steps given below:

1. Log on to Seqrite Terminator**>** **Settings > IPS> Advanced**. The Custom IPS screen is displayed.
2. To add IP addresses to White list 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.
4. Click **Save**. The IP address is added to the respective list.

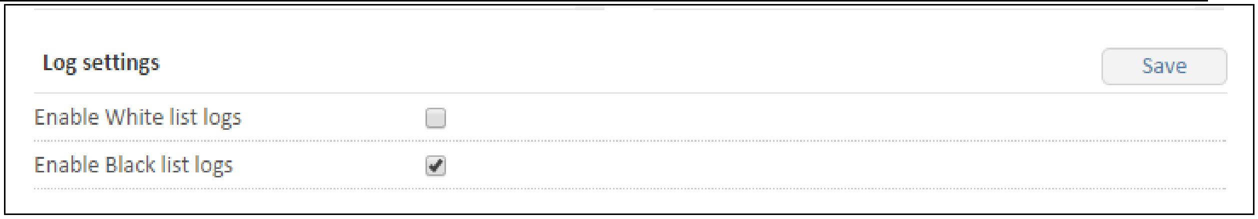
Removing IP addresses from the White / Black list

To remove IP addresses from whitelist /blacklist follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > IPS> Advanced**. The Custom IPS screen is displayed. 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**. The IP address will be removed from the respective list.
3. Click **Save**.

Enabling logs for White List/ Black List

1. Log on to Seqrite Terminator> **Settings** > **IPS**> **Advanced**. The Custom IPS screen is displayed.
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.



Log settings

Enable White list logs ☐

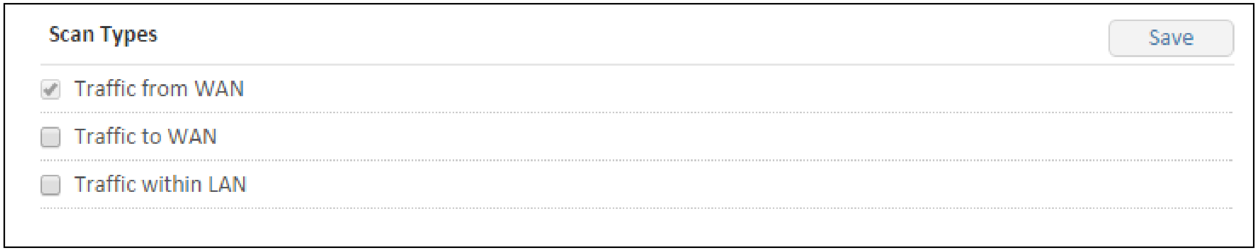
Enable Black list logs ☑

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. Log on to Seqrite Terminator **> Settings > IPS> Advanced**. The Custom IPS screen is displayed.
2. In the Scan Types area, select the type of traffic that you want the Terminator to scan.



Scan Types

☑ Traffic from WAN

☐ Traffic to WAN

☐ Traffic within LAN

By default in Terminator the scanning for Inbound Traffic that is traffic coming from WAN is selected.

3. Click **Save**.

Chapter

8

Device Management

Administrator

The Administration page on the Seqrite Terminator provides you the options to customize the look and feel of the Terminator, provide the landing message, and configure the time out for the sessions. The page also provides options for adding admin profiles, managing admin settings and SMTP settings.

The Admin page has the following sub-options:

- Date and Time: Change appliance Date and Time.
- Customize Portal: To customize the web portal as per your requirements.
- Admin Settings: To configure the appliance access, add admin users, and set password strength.
- Admin Profile: To add new Admin profiles with different levels for access.
- SMTP Settings: To configure the SMTP server parameters.

Date and Time setting

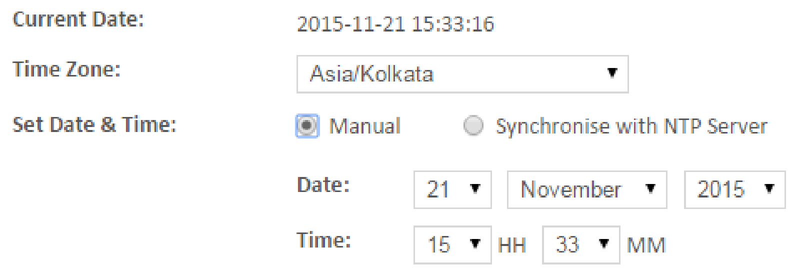
You can set the appliance date and time according to different geographical regions or synchronize with an NTP server.

To configure Date and Time settings, follow the steps given below:

1. Log in to your Seqrite Terminator **> Settings > Administration > Date & Time**.

   Following table explains the fields on page:

Field	**Description**
Current Time	Displays the current system time of the appliance.
Time Zone	Select time zone according to the geographical region in which the appliance is deployed.
Set Date &	Manual: Select the date and time from the dropdown.

Time	 Current Date: 2015-11-21 15:33:16 Time Zone: Asia/Kolkata ▾ Set Date & Time: ● Manual ○ Synchronise with NTP Server Date: 21 ▾ November ▾ 2015 ▾ Time: 15 ▾ HH 33 ▾ MM 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.

2. Click **Save**.

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

Admin Settings

You can control the appliance access ports and add users to the Administrative group. Using the Admin Setting page you can carry out the following tasks:

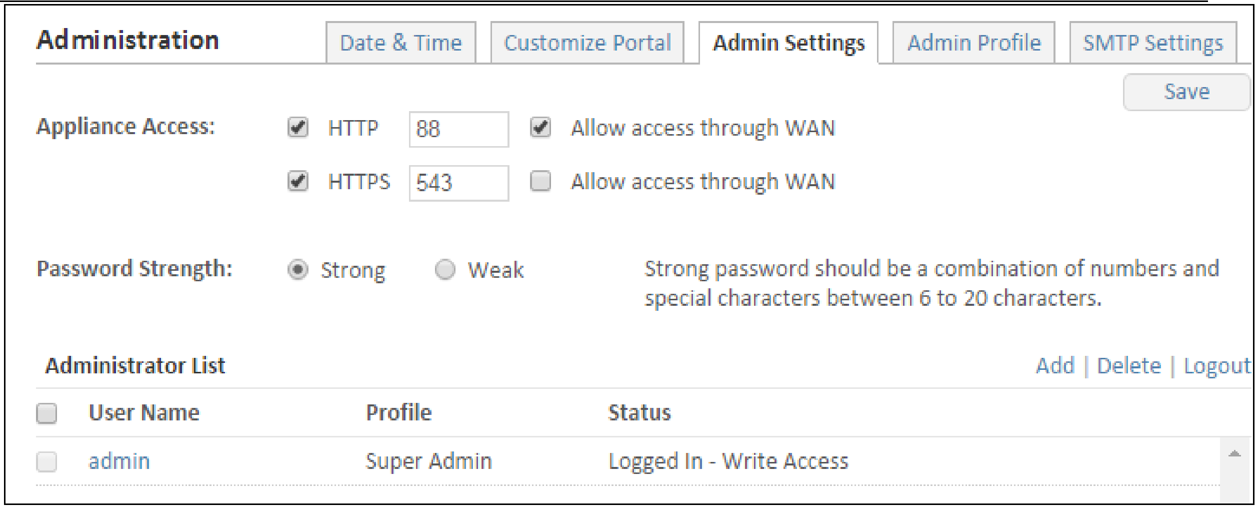
- Restrict access to the Terminator over WAN using the selected protocol.
- Set the password strength to be strong or weak.

  Note: The password strength settings are applicable to all the modules in the Terminator.
- Manage the administrators list, i.e. add, delete or force logout an admin user.

Configuring Administrator Access

To configure appliance access to admin follow the steps given below:

1. Log on to Seqrite Terminator **>Settings > Administration > Admin Settings**. The Admin settings page is displayed. The Administrators list on the page displays the number of users logged in as Administrators.



Appliance Access: ☑ HTTP 88 ☑ Allow access through WAN

☑ HTTPS 543 □ Allow access through WAN

Password Strength: ● Strong ○ Weak

Strong password should be a combination of numbers and special characters between 6 to 20 characters.

Administrator List

□	User Name	Profile	Status
□	admin	Super Admin	Logged In - Write Access

2. Select the type of access over WAN using the following fields:

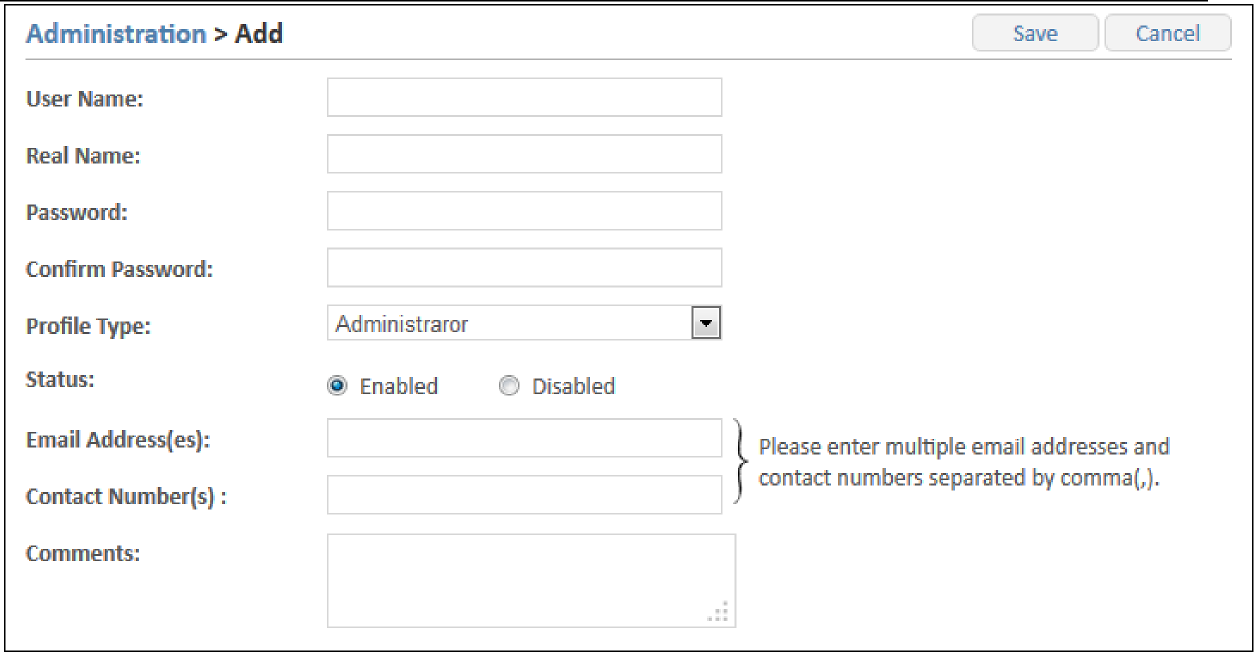
Field	Description
Protocol	Select at least one protocol from HTTP and HTTPS.
Port	Enter the port number(s) for accessing Terminator. By default it is 88, you can change this to any available port number.
WAN	Use this option to enable or disable appliance access over WAN using the selected protocol.

3. Select the **Password Strength** as required. A Strong password should be a combination of numbers and special characters between 6 to 20 characters.

Adding Administrators

To add an administrator follow the steps given below:

1. Log on to Seqrite Terminator **>Settings > Administration > Admin Settings**. The Admin settings page is displayed.
2. Click **Add** against the Administrator List. The Add Administrator page is displayed.



Administration > Add

User Name:

Real Name:

Password:

Confirm Password:

Profile Type: Administraror

Status: ● Enabled ○ Disabled

Email Address(es):

Contact Number(s) :

Please enter multiple email addresses and contact numbers separated by comma(,).

Comments:

The following table describes the fields on the page:

Field	Description
User Name	Enter the user name. Administrators use this username to log in to the Terminator.
Real Name	Enter the real name of an administrator user. Username and real name need not be the same.
Password	Enter the password.
Confirm Password	Re-enter the password to confirm.
Profile Type	Select profile type from drop-down list. Administrator: This admin user gets read and write access to the Terminator. Read Only: This admin gets read-only access to the Terminator. (See **Admin profile** for more details)
Status	Select a status of the Administrator. Administrator with disabled status will not be able to log in.
Email Address(es)	Enter comma separated list of email address (es).
Contact Number(s)	Enter comma separated list of contact number(s).

Field	Description
Comments	Enter the description for the admin user.

3. Click **Save**.

Deleting / logging out administrators

1. Log on to Seqrite Terminator as a Super Administrator **> Settings > Administration> Admin Settings**. The Admin settings page is displayed. The Administrators list displays the number of users logged in as Administrators.
2. Select the admin user that you want to delete / log out, click **Delete/Log out** as required.
3. Click **Save**.

Admin Profiles

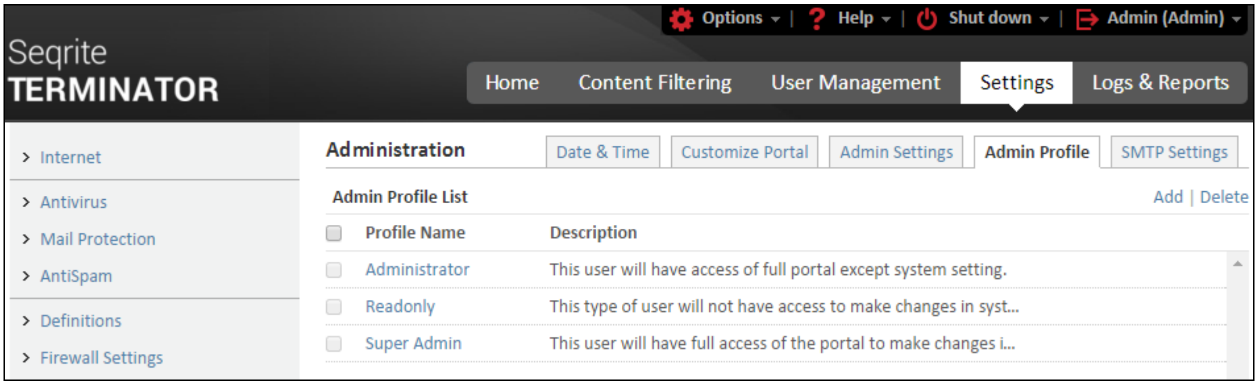
This section allows to manage web Admin profiles. It provides definition of the rights Admin user can have. You can create, edit and delete Admin profiles using this section. There are three predefined Admin profiles:

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.

These Admin profiles are displayed in the profile type list on the Add Administrator page as shown below.



Admin Profile List

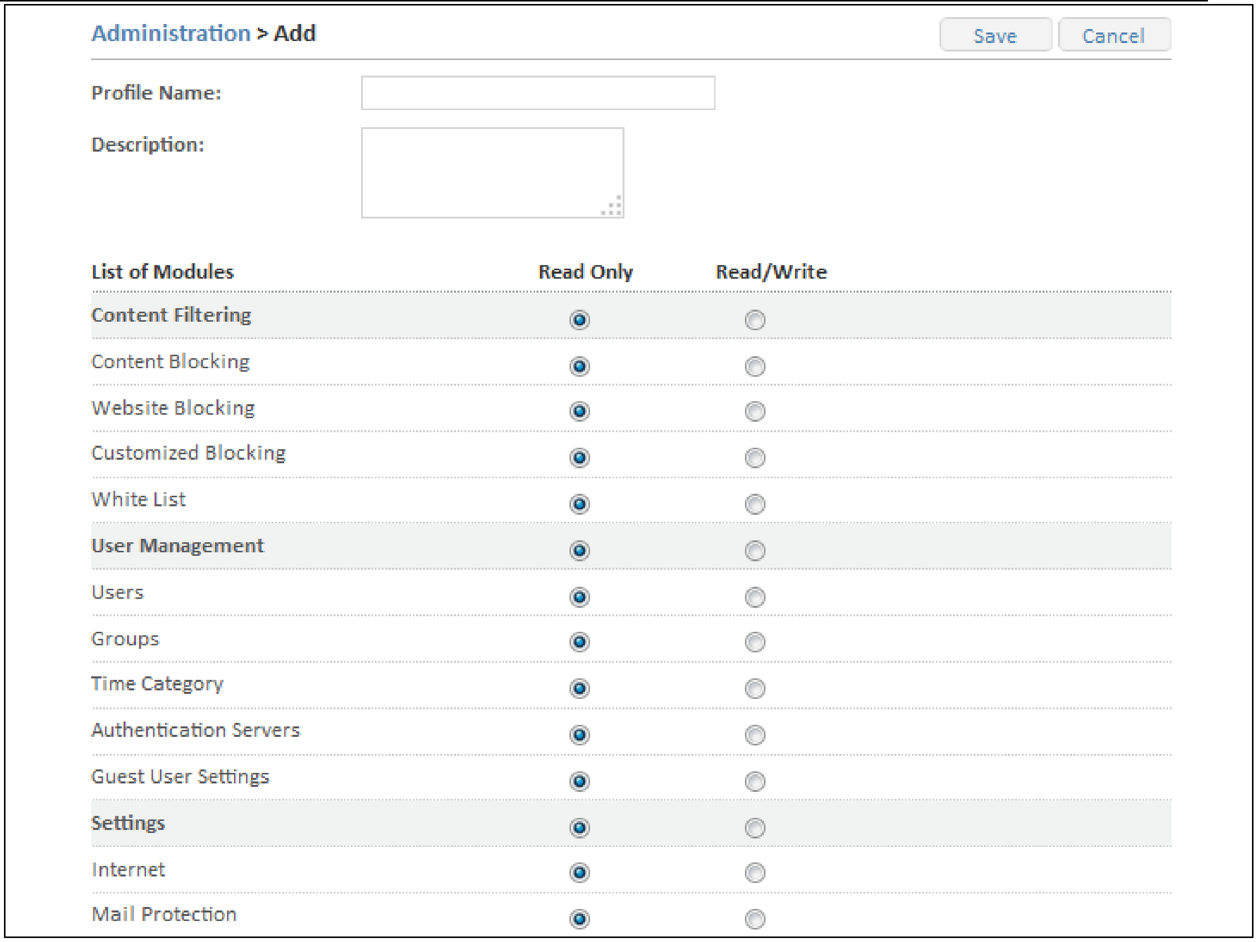
□	Profile Name	Description
□	Administrator	This user will have access of full portal except system setting.
□	Readonly	This type of user will not have access to make changes in syst...
□	Super Admin	This user will have full access of the portal to make changes i...

Creating Admin Profile

To create an Admin profile follow the steps given below:

1. Log on to Seqrite Terminator as a Super Administrator **> Settings > Administration > Admin Profile.**

2. Click **Add** to add a new Admin Profile. The List of modules is displayed.
3. Enter a **Profile name** for the new profile.
4. Enter a **Description** in the designated text box.



Profile Name:

Description:

List of Modules	Read Only	Read/Write
Content Filtering	●	○
Content Blocking	●	○
Website Blocking	●	○
Customized Blocking	●	○
White List	●	○
User Management	●	○
Users	●	○
Groups	●	○
Time Category	●	○
Authentication Servers	●	○
Guest User Settings	●	○
Settings	●	○
Internet	●	○
Mail Protection	●	○

5. Select the modules from the module list to which the new profile would have access. This list contains different right levels for the different modules of Terminator. Select to provide read-only or read-write access for the respective modules to the new Admin profile.

   Read only access: Allows to 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

1. Log on to Seqrite Terminator as a Super Administrator **> Settings > Administration > Admin Profile.**
2. Select the Admin profile that you want to delete, click **Delete**.

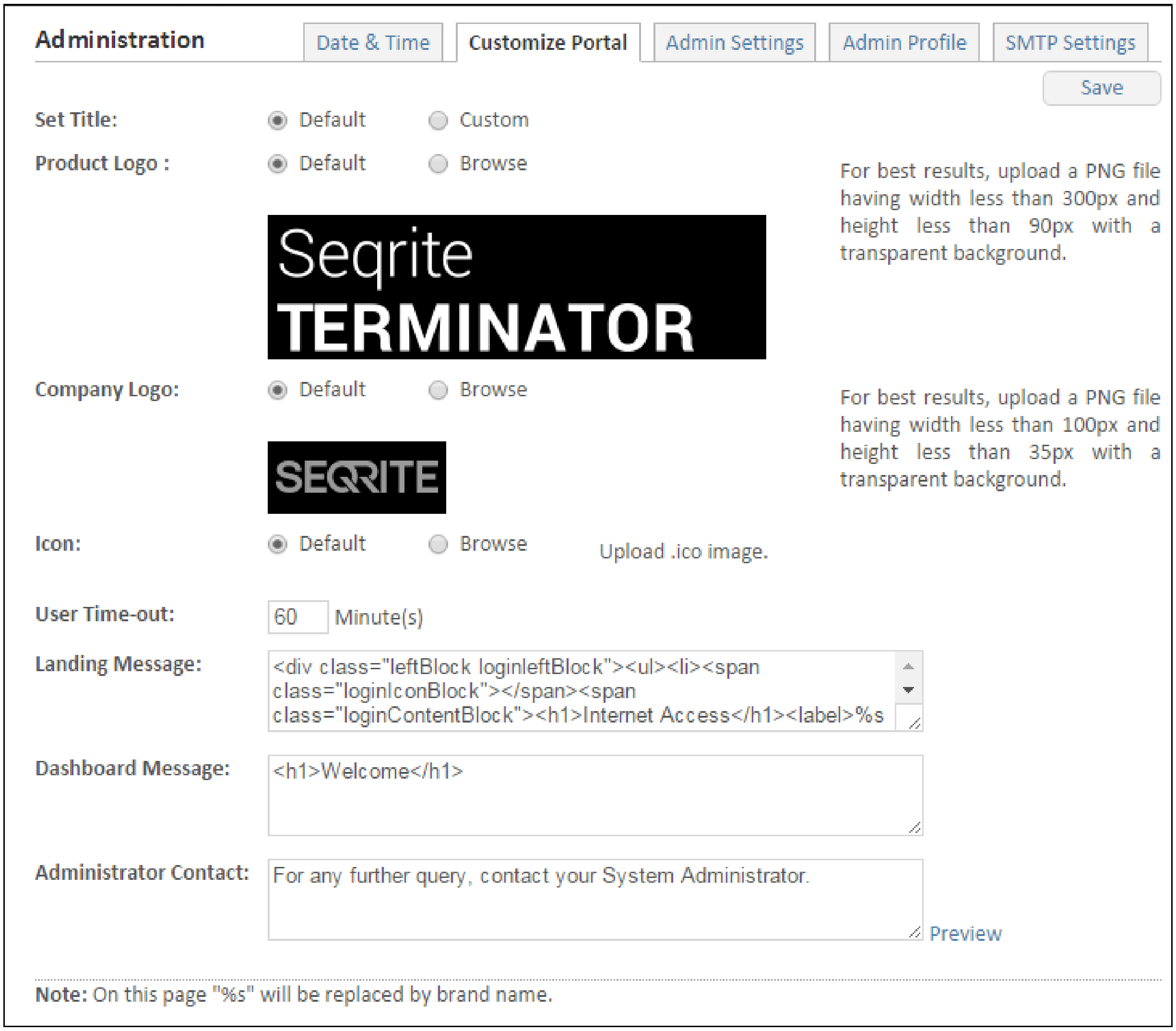
   Note: Deleted Admin profiles will be changed to Read-only user type. Predefined Admin profiles cannot be deleted.

Web Portal Customization

This feature allows you to customize Terminator web portal.

To customize web portal, follow the steps given below: interrupt

1. Log on to Seqrite Terminator **> Settings > Administration**. By default the Customize portal page is displayed.



Administration

Set Title: ● Default ○ Custom

Product Logo : ● Default ○ Browse

For best results, upload a PNG file having width less than 300px and height less than 90px with a transparent background.

Company Logo: ● Default ○ Browse

For best results, upload a PNG file having width less than 100px and height less than 35px with a transparent background.

Icon: ● Default ○ Browse Upload .ico image.

User Time-out: 60 Minute(s)

Landing Message:

```
<div class="leftBlock loginleftBlock"><ul><li><span
class="loginIconBlock"></span><span
class="loginContentBlock"><h1>Internet Access</h1><label>%s
```

Dashboard Message:

```
<h1>Welcome</h1>
```

Administrator Contact: For any further query, contact your System Administrator.

Note: On this page "%s" will be replaced by brand name.

2. The below table describes the fields on the page:

Field	Description
Set Title	The site title might be the name of your company or organization, or a brief description of the organization, or a combination of the two. This title can be modified using custom option or can be set to default. It should *not be blank and should be alphanumeric.*

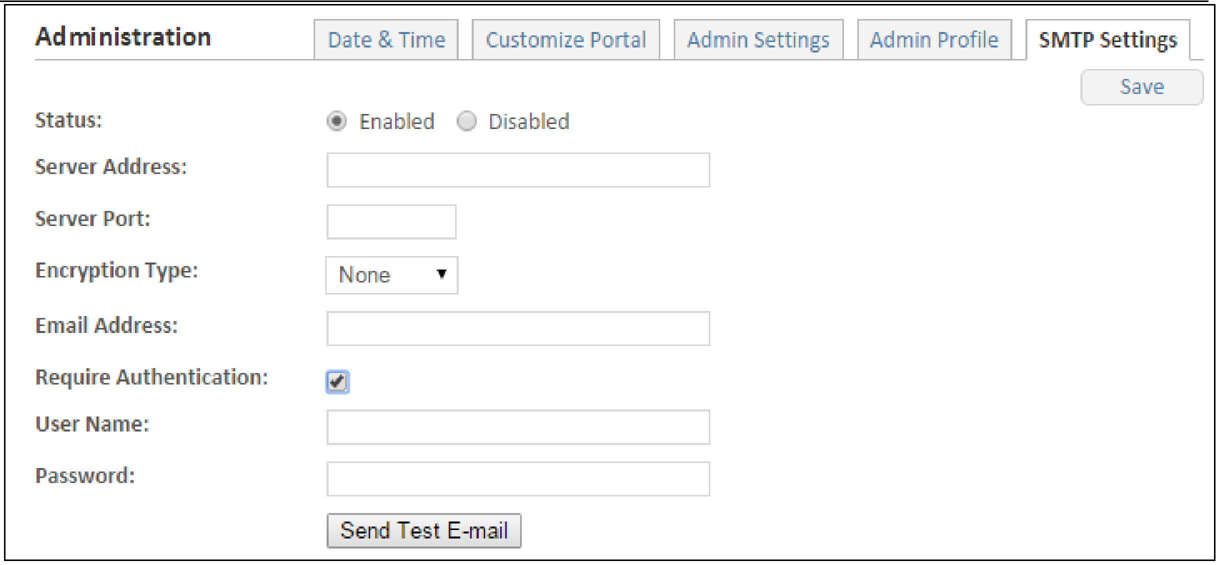
Field	Description
Product Logo	Using this option, administrator can set default logo or can upload new logo for user web portal. *This logo should have transparent background and dimensions should be 300X90 pixels.*
Company Logo	Using this option, administrator can set a default logo for Company or can upload new logo for user web portal. *This logo should have transparent background and dimensions should be 100X35 pixels. Company logo will appear in footer.*
Icon (favicon)	There are two options default and custom. Using this option, administrator can set default favicon or can upload a new favicon for user web portal.
User Time-out	Using this option, you can set default idle session time-out for user in minutes.
Landing Message	One approach to writing a Web site landing message is to provide a brief statement of the purpose of your Web site. This message displays on login page before user logs in.
Dashboard Message	This message is shown when user logs in to the web portal.
Administrator Contact	Details for administrator can be provided. This message is shown on error pages. Administrator can customize this message.

3. Click **Save**.

SMTP Settings

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

1. Log on to Seqrite Terminator as a Super Administrator > **Settings** > **Administration** > **SMTP settings**.



Status: ● Enabled ○ Disabled

Server Address:

Server Port:

Encryption Type: None ▾

Email Address:

Require Authentication: ☑

User Name:

Password:

The following table describes the fields on page:

Field	Description
Status	Select 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.
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.
User Name	Enter the User Name. It should be valid email address. Username and password is required for SMTP server authentication.
Password	Enter the password. This is the password of the email account that you have configured to receive email notification.

2. Click **Save**.

Updates

You can manage the Terminator service and system updates using the Updates page. The Service updates include Antivirus and IPS/IDS signature updates whereas system updates includes the stability / bug fixes.

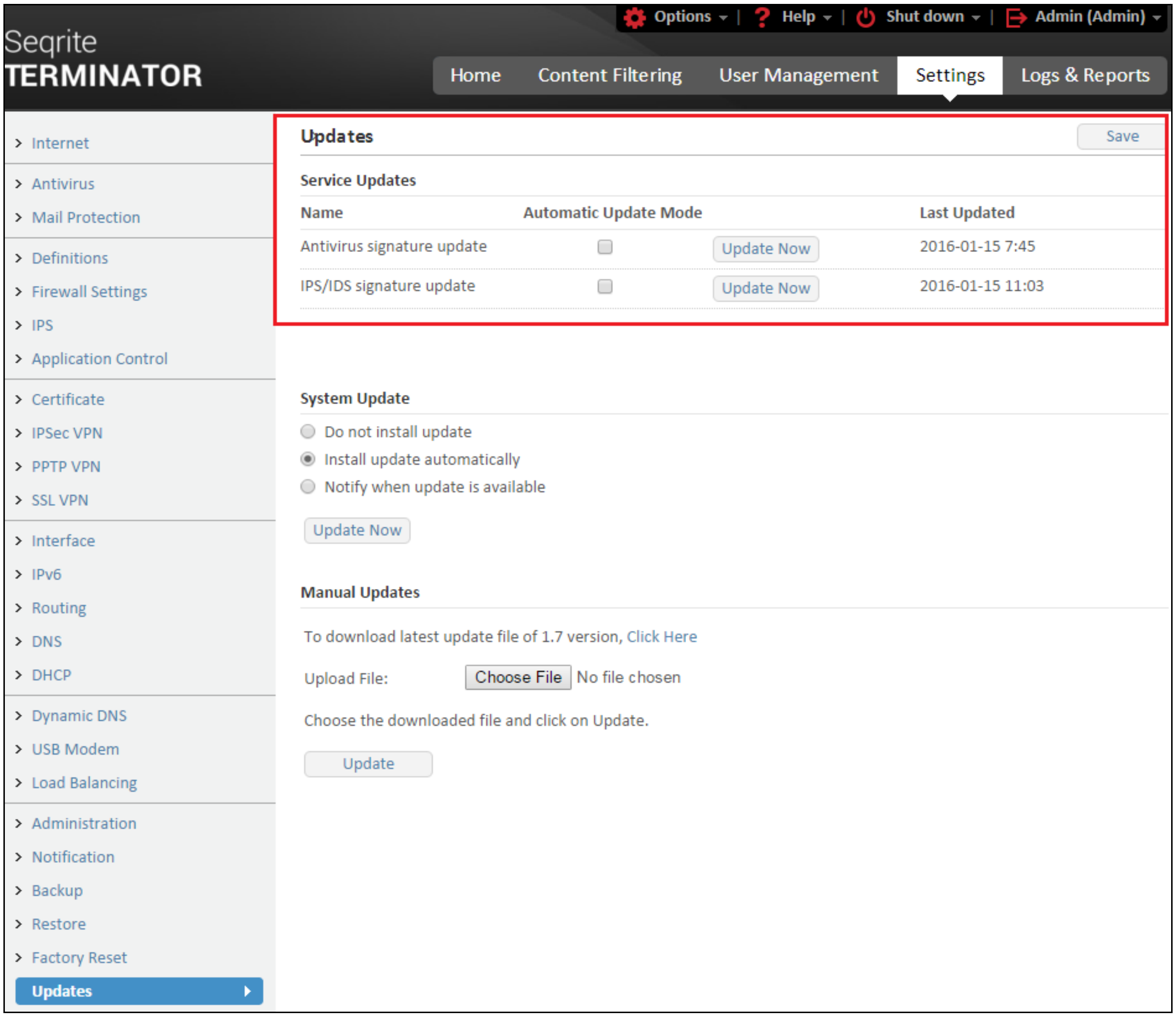
You can set the Service updates to be done automatically or update it whenever you wish to using the Update Now button. You can also set the System Updates to be installed automatically, as well as get notifications about the update and then install the updates as per your convenience.

The Updates page also allows you to manually update the Terminator by downloading the latest update file from the Seqrite website and then uploading it.

Configuring Service Updates

To configure Service Updates follow these steps:

1. Log on to Seqrite Terminator **> Settings > Updates**.



Updates

Service Updates

Name	Automatic Update Mode		Last Updated
Antivirus signature update	□	Update Now	2016-01-15 7:45
IPS/IDS signature update	□	Update Now	2016-01-15 11:03

System Update

○ Do not install update
● Install update automatically
○ Notify when update is available

Update Now

Manual Updates

To download latest update file of 1.7 version, Click Here

Upload File: Choose File No file chosen

Choose the downloaded file and click on Update.

Update

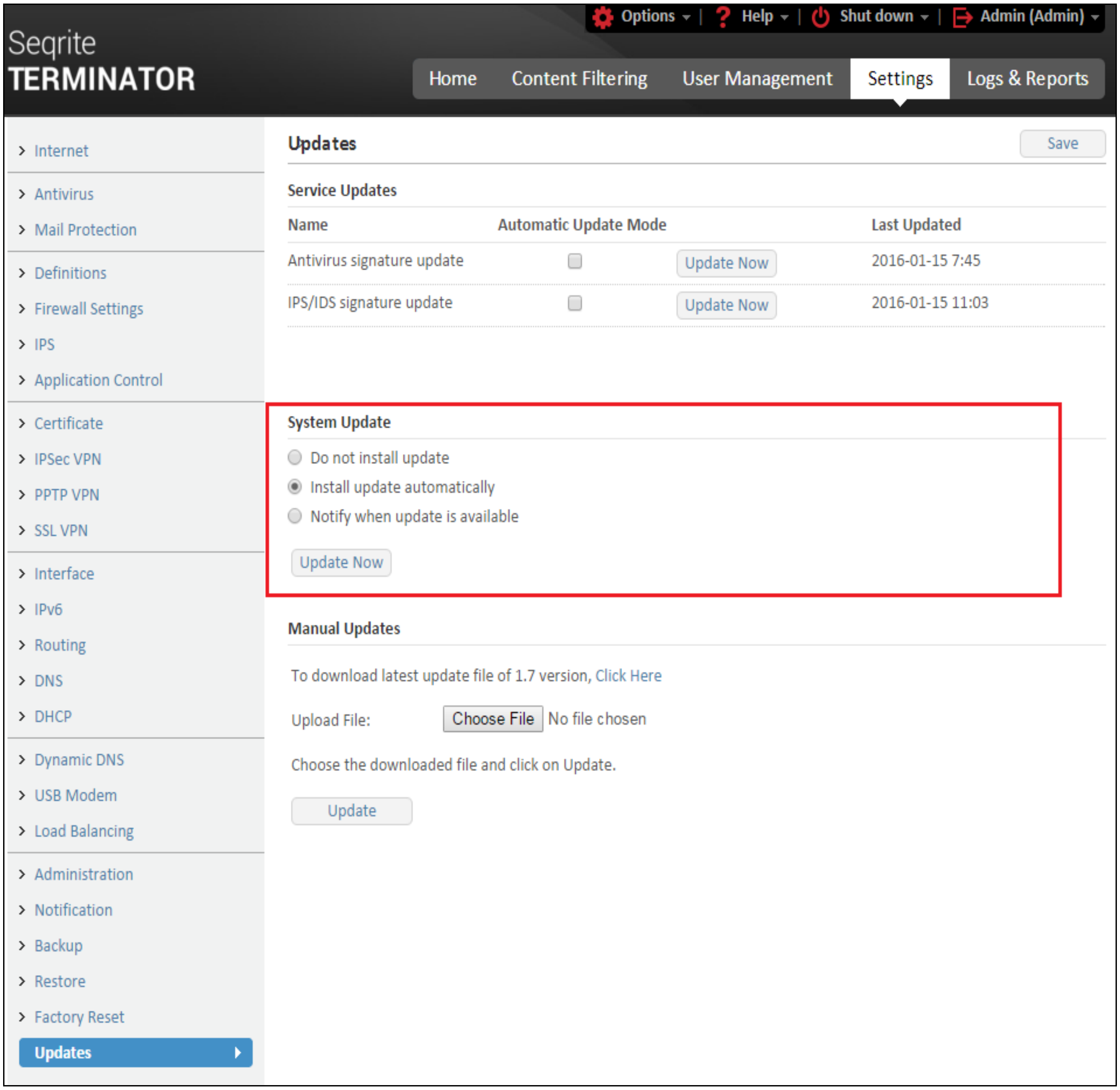
2. Click on/off button to enable/disable the automatic update mode for the respective services.

3. Click on **Update Now** button to install the available updates for the particular service.

Configuring System Updates

To configure System Updates follow these steps:

1. Log on to Seqrite Terminator **> Settings > Updates**.



Updates

Service Updates

Name	Automatic Update Mode		Last Updated
Antivirus signature update	□	Update Now	2016-01-15 7:45
IPS/IDS signature update	□	Update Now	2016-01-15 11:03

System Update

○ Do not install update
● Install update automatically
○ Notify when update is available

Update Now

Manual Updates

To download latest update file of 1.7 version, Click Here

Upload File: Choose File No file chosen

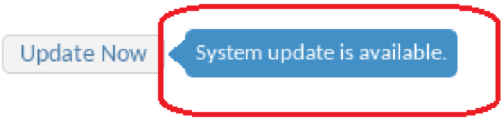
Choose the downloaded file and click on Update.

Update

2. You can select the following options for system updates:

- **Do not install update**: System updates will not be installed.

- **Install updates automatically**: System updates will be checked after an interval of 4 hours and if there is any update available then the system will be installed automatically.
- **Notify when update is available**: Notification about the system update will be displayed.



System update is available.

- Click on the Update Now button to install the system updates if available.

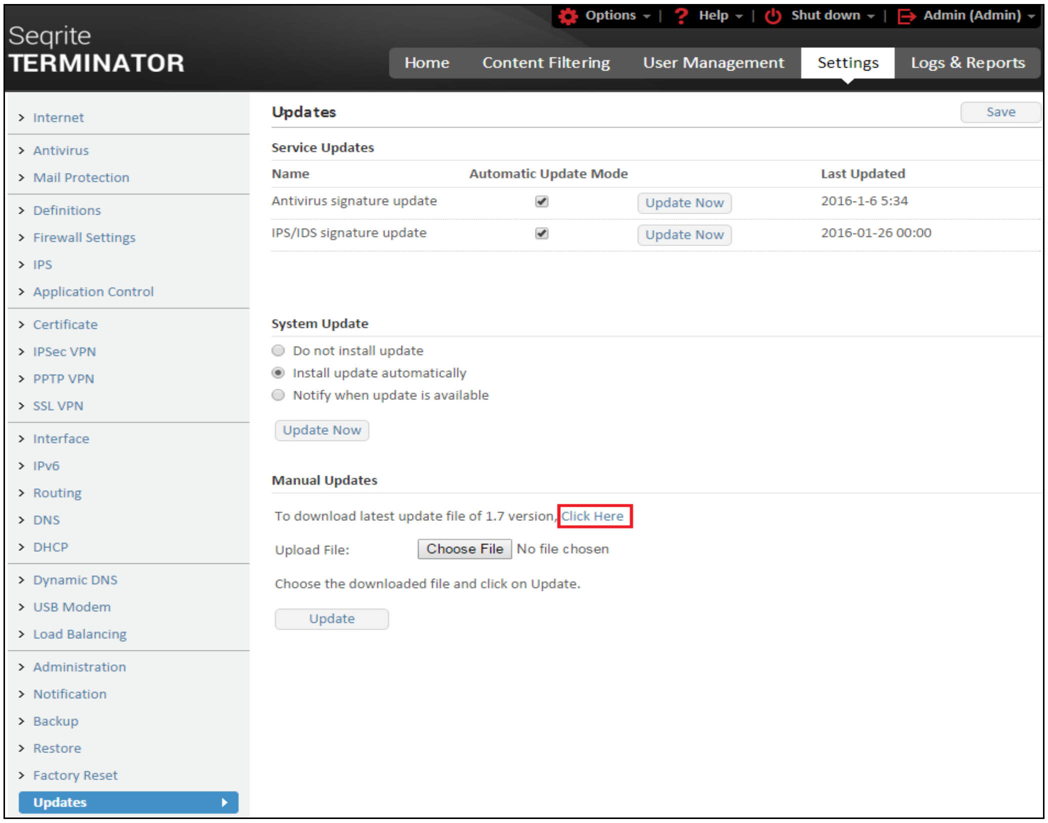
Configuring Manual Updates

To configure the manual updates, follow these steps:

1. Log on to Seqrite Terminator **> Settings > Updates.**
2. Download the update file by clicking the **Click here** link in the Manual Update section. Or you can also paste the following link in your browser.

   http://www.seqrite.com/seqrite-offline-product-updates

   Note: For downloading the update files you need an internet connection.



Updates

Service Updates

Name	Automatic Update Mode		Last Updated
Antivirus signature update	☑	Update Now	2016-1-6 5:34
IPS/IDS signature update	☑	Update Now	2016-01-26 00:00

System Update

○ Do not install update
● Install update automatically
○ Notify when update is available

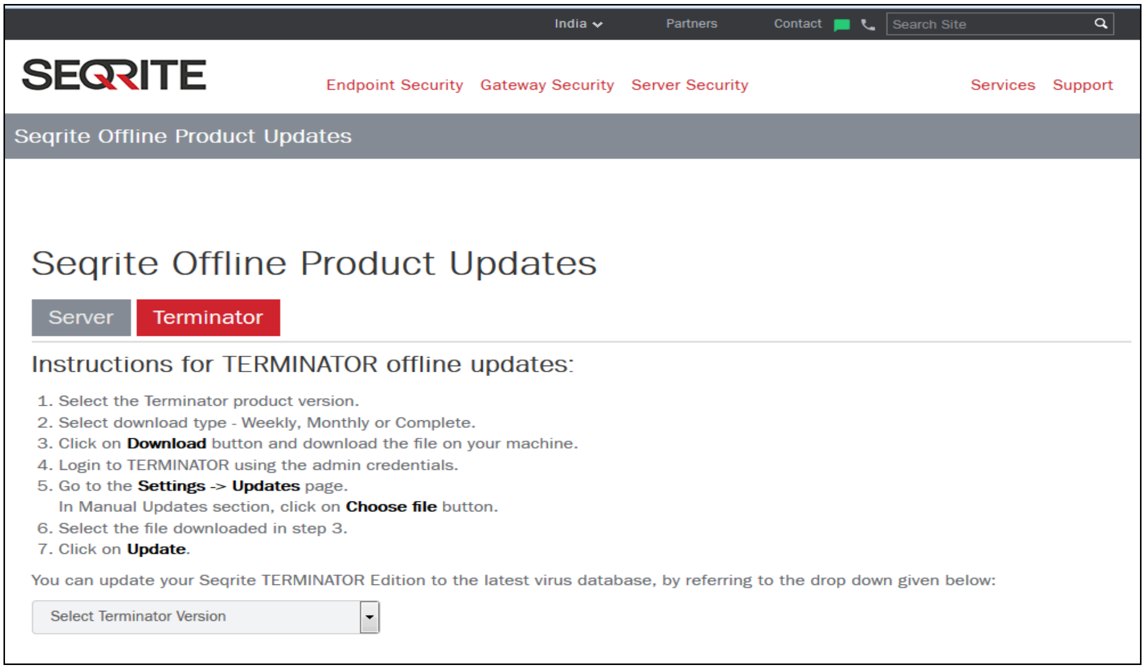
Manual Updates

To download latest update file of 1.7 version, Click Here

Upload File: Choose File No file chosen

Choose the downloaded file and click on Update.

The Seqrite offline update website is opened.



Seqrite Offline Product Updates

Instructions for TERMINATOR offline updates:

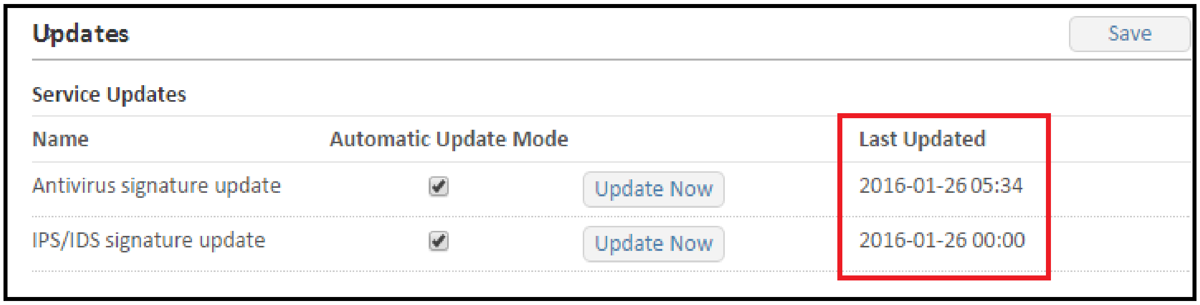
1. Select the Terminator product version.
2. Select download type - Weekly, Monthly or Complete.
3. Click on **Download** button and download the file on your machine.
4. Login to TERMINATOR using the admin credentials.
5. Go to the **Settings** -> **Updates** page.
   In Manual Updates section, click on **Choose file** button.
6. Select the file downloaded in step 3.
7. Click on **Update**.

You can update your Seqrite TERMINATOR Edition to the latest virus database, by referring to the drop down given below:

3. Click on the **Terminator** tab.

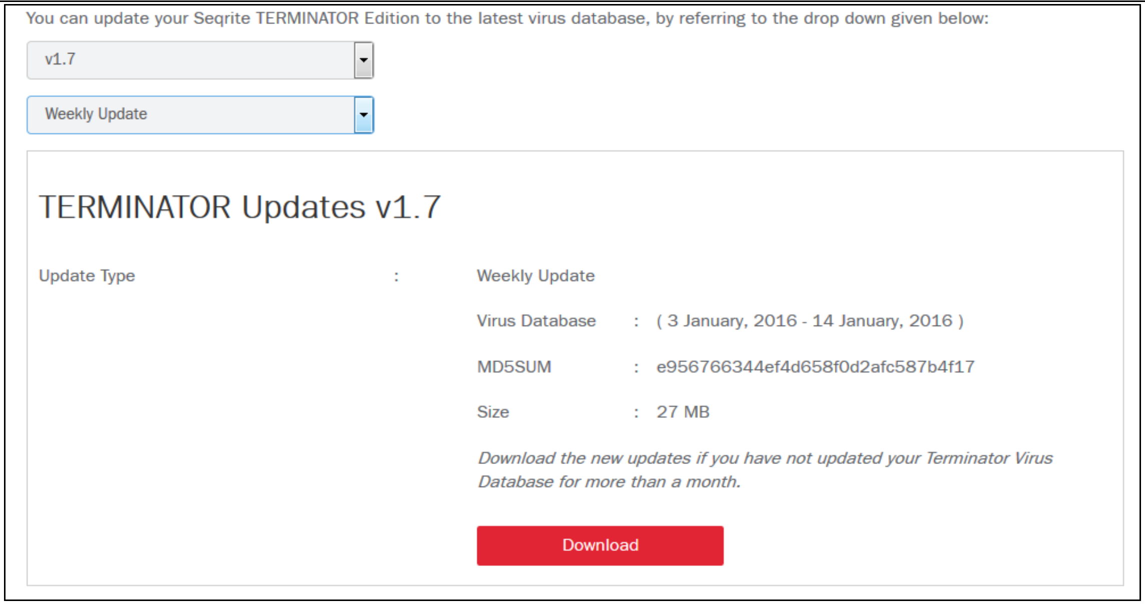
4. Select the **Terminator Version**.

5. Select the type of update from weekly, monthly and complete. This depends on the last updates taken. Select the appropriate update type according to the Last Updated date displayed in the **Service Update** section.



Name	Automatic Update Mode		Last Updated
Antivirus signature update	☑	Update Now	2016-01-26 05:34
IPS/IDS signature update	☑	Update Now	2016-01-26 00:00

If the Last Updated date falls in the weekly range, then download the weekly update file. Similarly you can check for monthly update. Incase if the last updated date does not fit in the weekly or monthly update range then select the Complete update file.



You can update your Seqrite TERMINATOR Edition to the latest virus database, by referring to the drop down given below:

TERMINATOR Updates v1.7

Update Type : Weekly Update

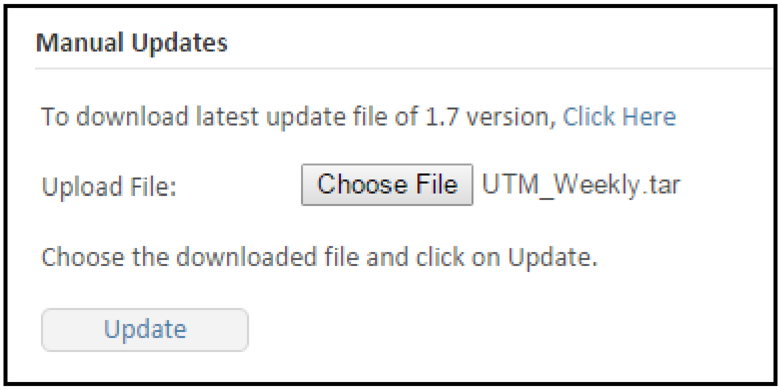
Virus Database : (3 January, 2016 - 14 January, 2016)

MD5SUM : e956766344ef4d658f0d2afc587b4f17

Size : 27 MB

Download the new updates if you have not updated your Terminator Virus Database for more than a month.

6. Click **Download**. A tar file will be downloaded.
7. In the **Manual Updates** section on the Updates page choose the file and click **Update**.



Manual Updates

To download latest update file of 1.7 version, Click Here

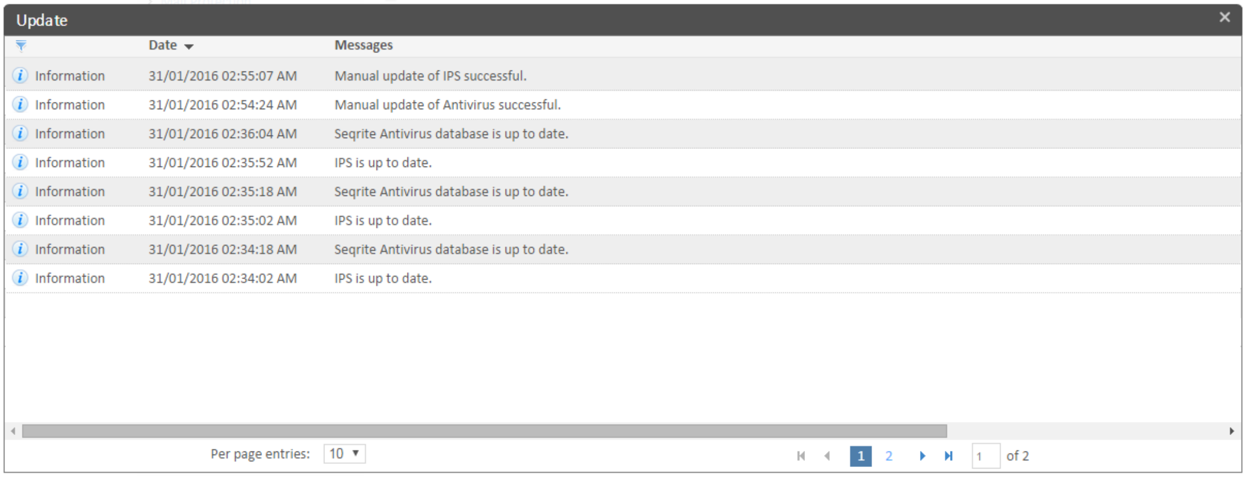
Upload File: UTM_Weekly.tar

Choose the downloaded file and click on Update.

Note:

- The file extension should not be changed.
- Incase of insufficient space on device, extract the update files and upload individually.

8. Wait till the update process is completed.
9. Once the manual update process is completed a message is displayed, informing if the manual update was successful or failed.
10. You can also go **to Logs & Reports > Log Viewer > Updates** and confirm.



Update

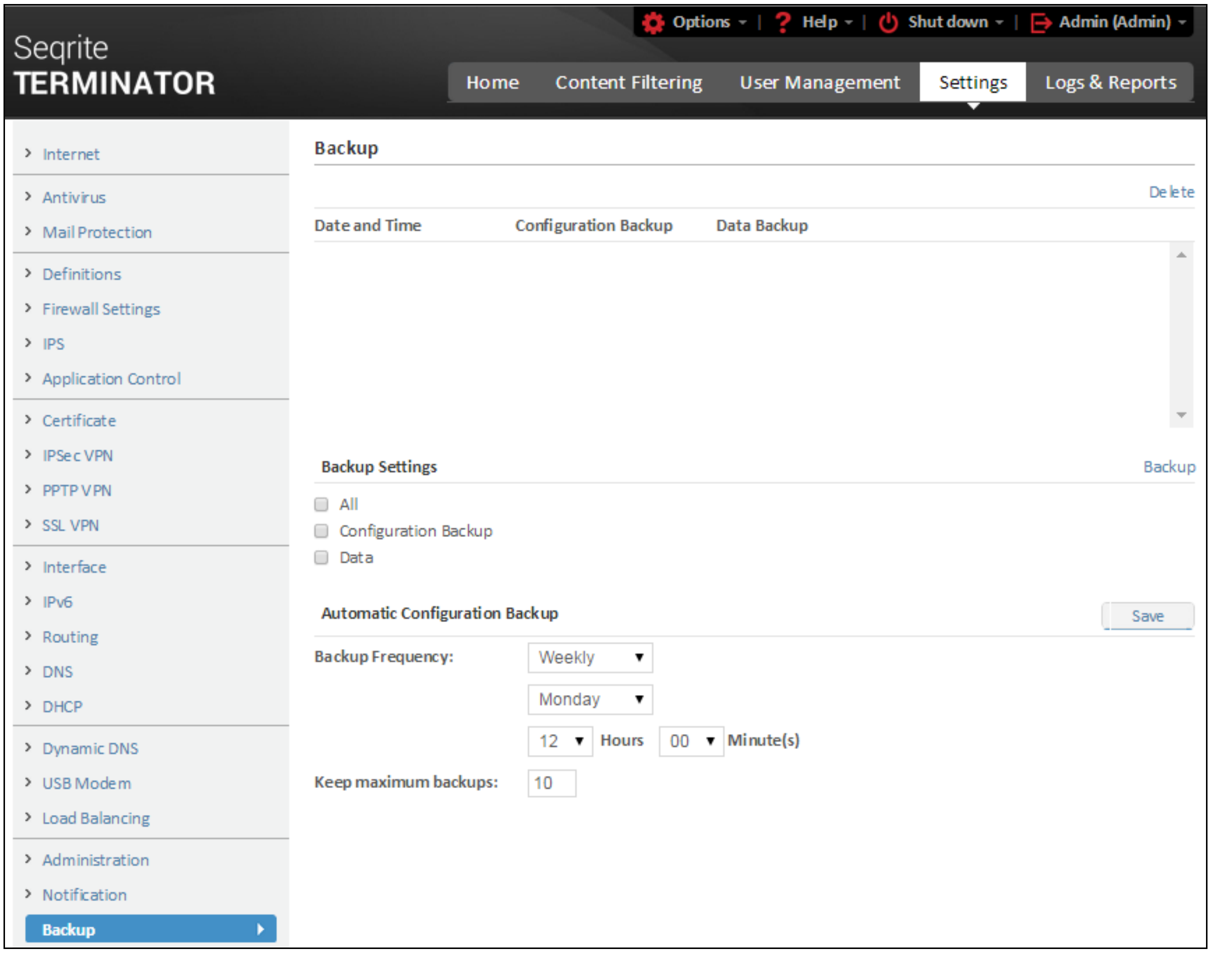
	Date	Messages
Information	31/01/2016 02:55:07 AM	Manual update of IPS successful.
Information	31/01/2016 02:54:24 AM	Manual update of Antivirus successful.
Information	31/01/2016 02:36:04 AM	Seqrite Antivirus database is up to date.
Information	31/01/2016 02:35:52 AM	IPS is up to date.
Information	31/01/2016 02:35:18 AM	Seqrite Antivirus database is up to date.
Information	31/01/2016 02:35:02 AM	IPS is up to date.
Information	31/01/2016 02:34:18 AM	Seqrite Antivirus database is up to date.
Information	31/01/2016 02:34:02 AM	IPS is up to date.

Backup and Restore

Seqrite Terminator allows to take backup of the settings, configuration and data which can help in case the Terminator crashes or if you want to revert to the previous settings. You can take backup of Terminator default settings, user defined settings, and user database settings and stores it to reuse in case of any technical emergency.

In order to take a backup follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > Backup**. The Backup settings page is displayed.



Backup

Date and Time	Configuration Backup	Data Backup

Backup Settings

□ All

□ Configuration Backup

□ Data

Automatic Configuration Backup

Backup Frequency: Weekly ▼

Monday ▼

12 ▼ Hours 00 ▼ Minute(s)

Keep maximum backups: 10

2. Select the type of backup you want to take. These can be as follows:

Type	Description
All	Takes backup of both Terminator configurations and reports.
Configuration	Takes backup of Terminator configurations (except Interface and Static route).
Data	Takes backup of Reports (except Log Viewer).

3. Click **Backup**. The Backup is taken on the internal CF Flash card.

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.

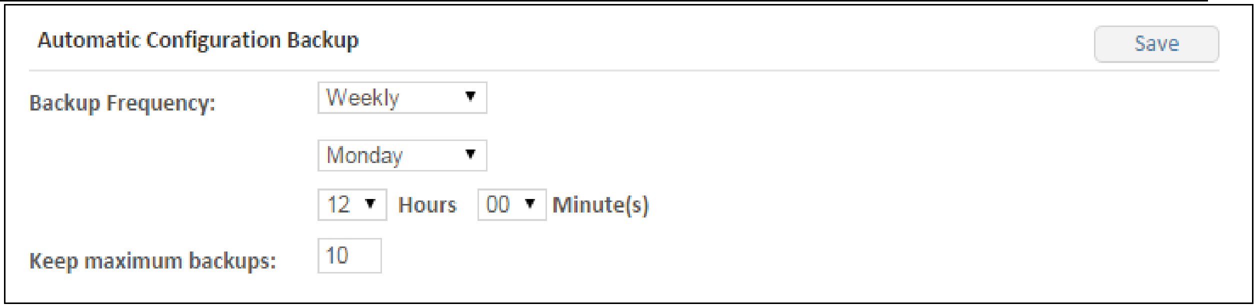
Automatic Configuration Backup

This feature allows you to set the Terminator 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.

To set Automatic Configuration Backup follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > Backup**. The Backup settings page is displayed.
2. Under **Automatic Configuration Backup** set the frequency of the backup to be taken.



Automatic Configuration Backup

Backup Frequency: Weekly ▼

Monday ▼

12 ▼ Hours 00 ▼ Minute(s)

Keep maximum backups: 10

3. Select the **Backup frequency**: This can be as follows:

Frequency	Description
None	Disables the automatic backup. On selecting this option Terminator will not take any backup.
Daily	Sets the Terminator to take the backup daily at a selected time period. Select the time in hours & minutes to take the backup daily.
Weekly	Sets the Terminator to take backup once in a week. Select the weekday & time in hours & minutes to take the backup. This is the default option and backup will be taken on every Monday at 12:00 PM (IST).
Monthly	Sets the Terminator to take backup once in a month. Select the day of month & time in hours & minutes when you want the backup to be taken.

4. Enter the maximum number of backups that can be stored on the Terminator in the **Keep maximum backups** field:

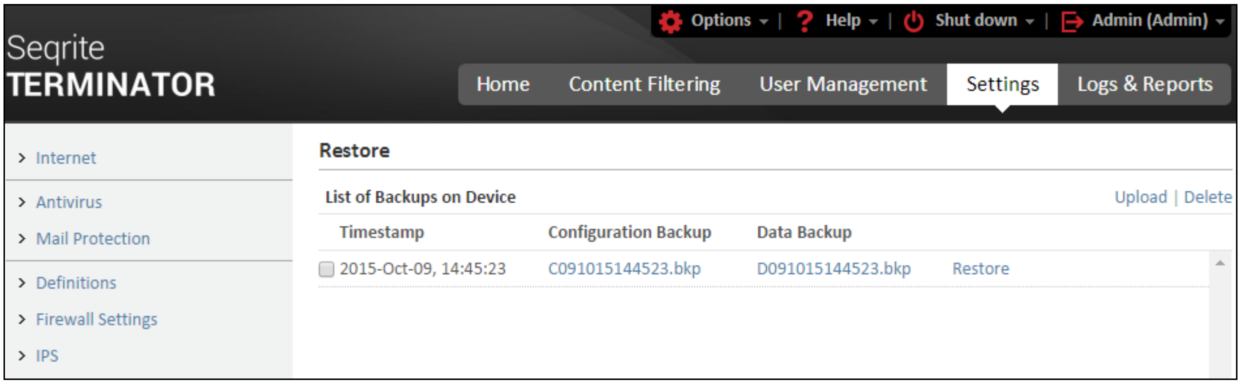
   The maximum number of backups can be less than or equal to 100. If the number of backup reaches this limit the oldest backup will be deleted automatically.

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 Terminator. You can restore the Terminator Configurations and Reports using the Restore option.

To restore backup follow the steps given below:

1. Log on to Seqrite **Terminator > Settings > Restore**. The Restore settings page is displayed with a list of all previously taken backups with the time, date and the type of backup.

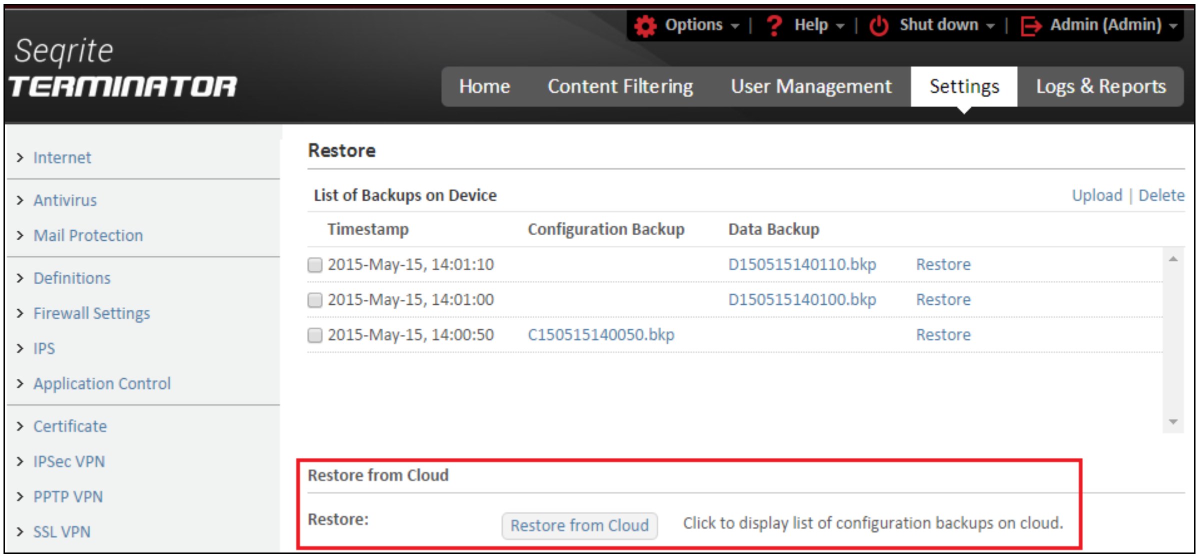


Restore

List of Backups on Device

	Timestamp	Configuration Backup	Data Backup	
□	2015-Oct-09, 14:45:23	C091015144523.bkp	D091015144523.bkp	Restore

2. Select the type of backup you want to restore and click **Restore**. You can also upload a backup file that was previously downloaded using the Backup option. Use the **Upload** buttons to browse and upload a backup file.
3. You can also restore backup from Cloud incase you have enabled Cloud service.
4. Click **Restore from cloud** option on the Restore page as shown in the following figure:



Restore

List of Backups on Device

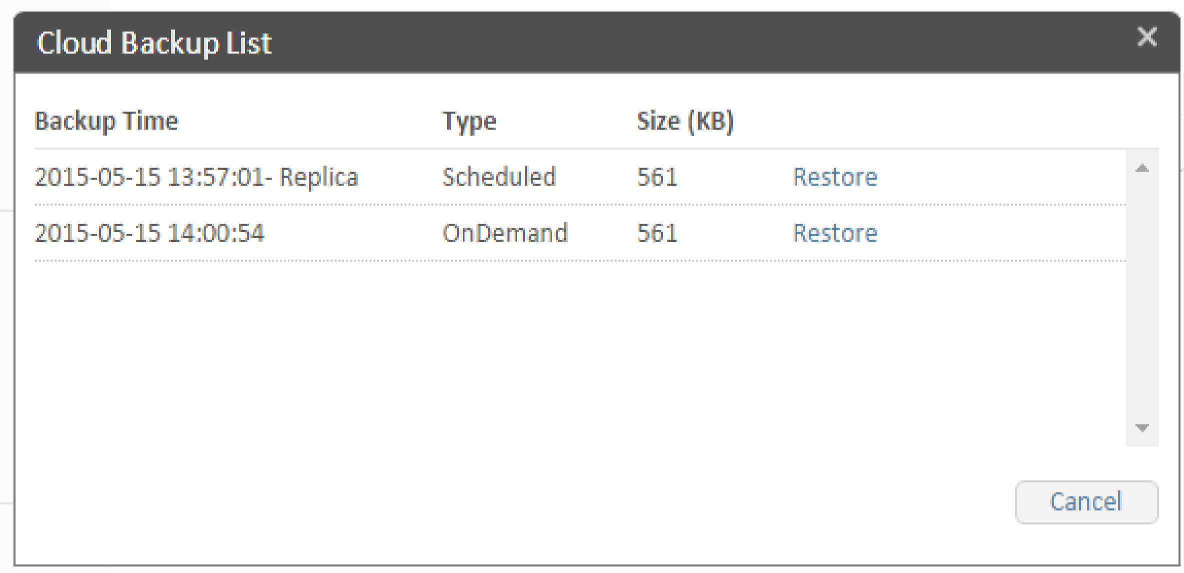
	Timestamp	Configuration Backup	Data Backup	
□	2015-May-15, 14:01:10		D150515140110.bkp	Restore
□	2015-May-15, 14:01:00		D150515140100.bkp	Restore
□	2015-May-15, 14:00:50	C150515140050.bkp		Restore

Restore from Cloud

Restore: Restore from Cloud Click to display list of configuration backups on cloud.

5. The Cloud backup list popup is displayed. This list contains the following backups:
   - Replica: This is the default backup, which is automatically updated on cloud whenever there is configuration change on Terminator.

- On demand: This is the manual backup taken for **All** that is configuration and data backup.



Cloud Backup List

Backup Time	Type	Size (KB)	
2015-05-15 13:57:01- Replica	Scheduled	561	Restore
2015-05-15 14:00:54	OnDemand	561	Restore

6. Click **Restore** against the backup you want to restore.

Deleting a backup

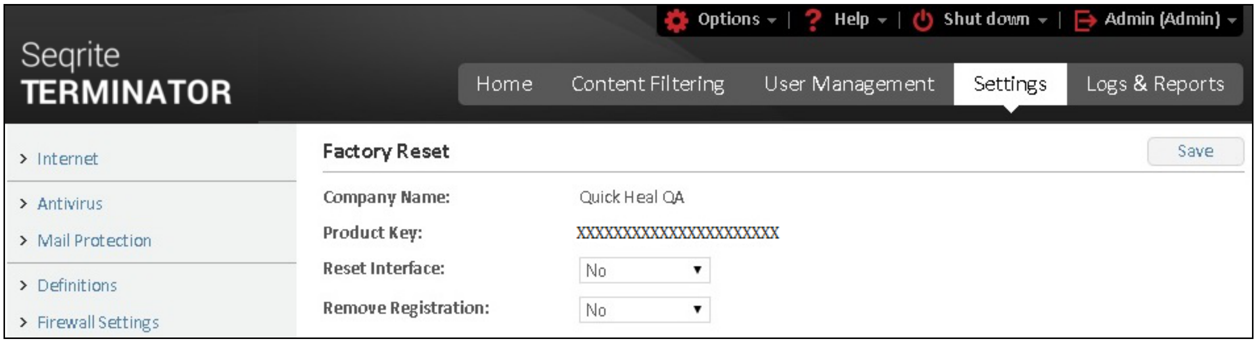
To delete a backup follow the steps given below:

1. Log on to Seqrite Terminator> **Settings** > **Restore**.
2. Select the backup you want to delete and click **Delete**. The selected backup is deleted.

Factory reset

With the factory reset, the Terminator 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 Terminator Settings, User Defined Settings, and reports will be lost.

1. Log on to Seqrite Terminator **> Settings > Factory Reset**. The Factory reset screen is displayed.



Factory Reset

Company Name:	Quick Heal QA
Product Key:	XXXXXXXXXXXXXXXXXXXXXX
Reset Interface:	No
Remove Registration:	No

2. Select whether you want to reset the interface, if you select **YES**, the current IP address is flushed and the default IP of Terminator is taken.
3. Select whether you want to remove the registration, if you select **YES**, the Terminator’s registration will be removed. You need to register Terminator again in order to use it.
4. Click **Save**.

License Details

The License Details page displays the license information about the Terminator. It includes the following details:

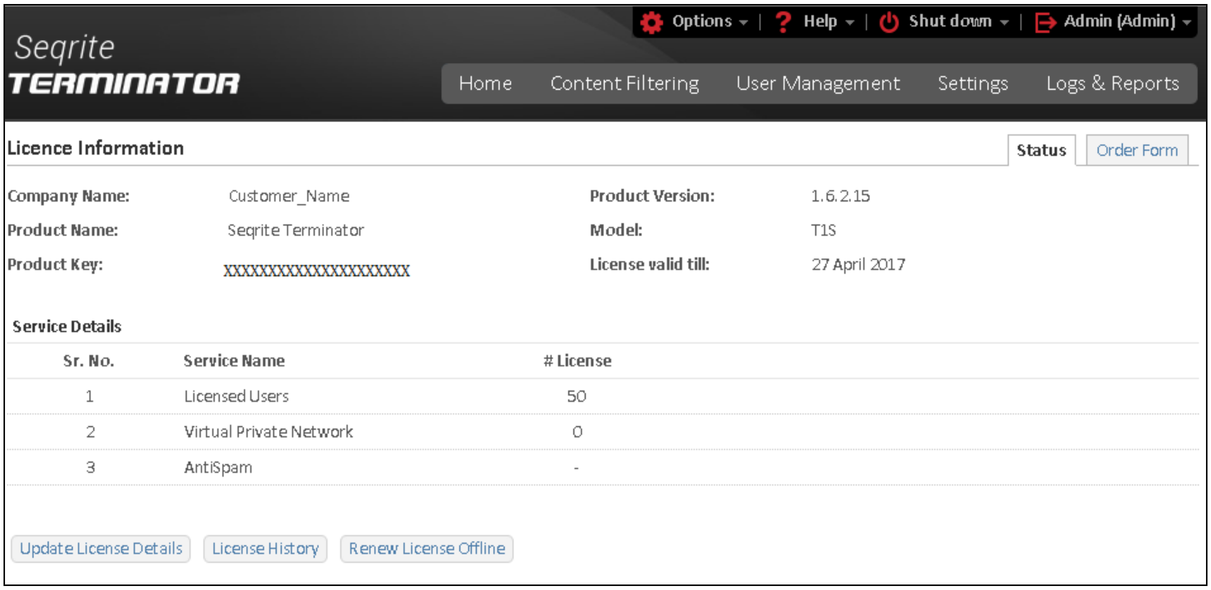
License details: This includes the company name, product name, product key, product version, model and license expiry date.

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.

To view license details follow these steps:

1. Log in to Seqrite Terminator **> Help > License Details.**
2. The License Details page is displayed.



Licence Information

Company Name:	Customer_Name	Product Version:	1.6.2.15
Product Name:	Seqrite Terminator	Model:	T1S
Product Key:	XXXXXXXXXXXXXXXXXXXXX	License valid till:	27 April 2017

Service Details

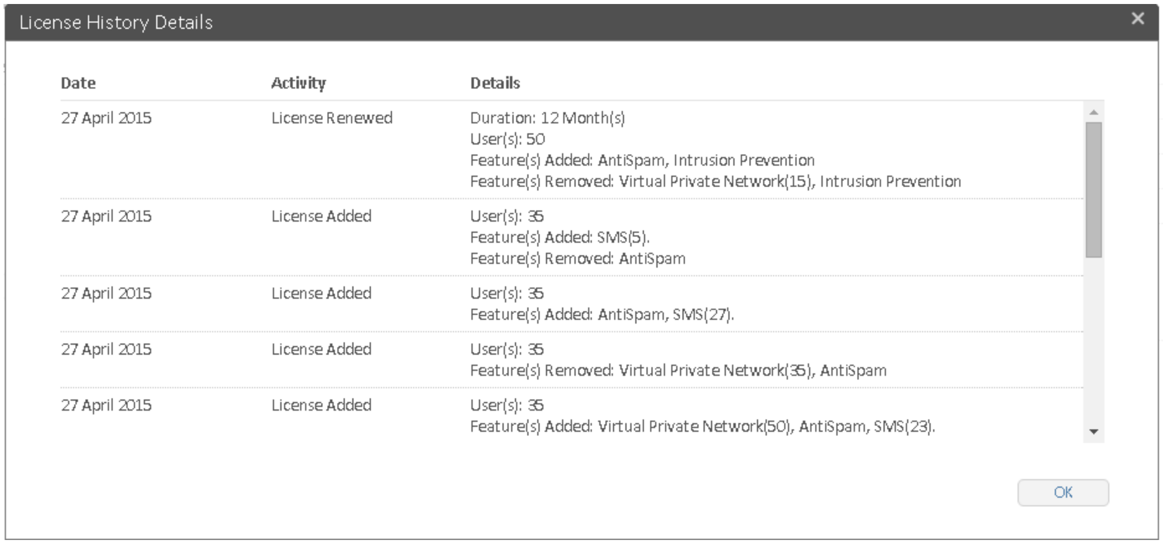
Sr. No.	Service Name	# License
1	Licensed Users	50
2	Virtual Private Network	0
3	AntiSpam	-

Following table explains the field 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 Terminator.
Model	Displays the model type of the Terminator.
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.

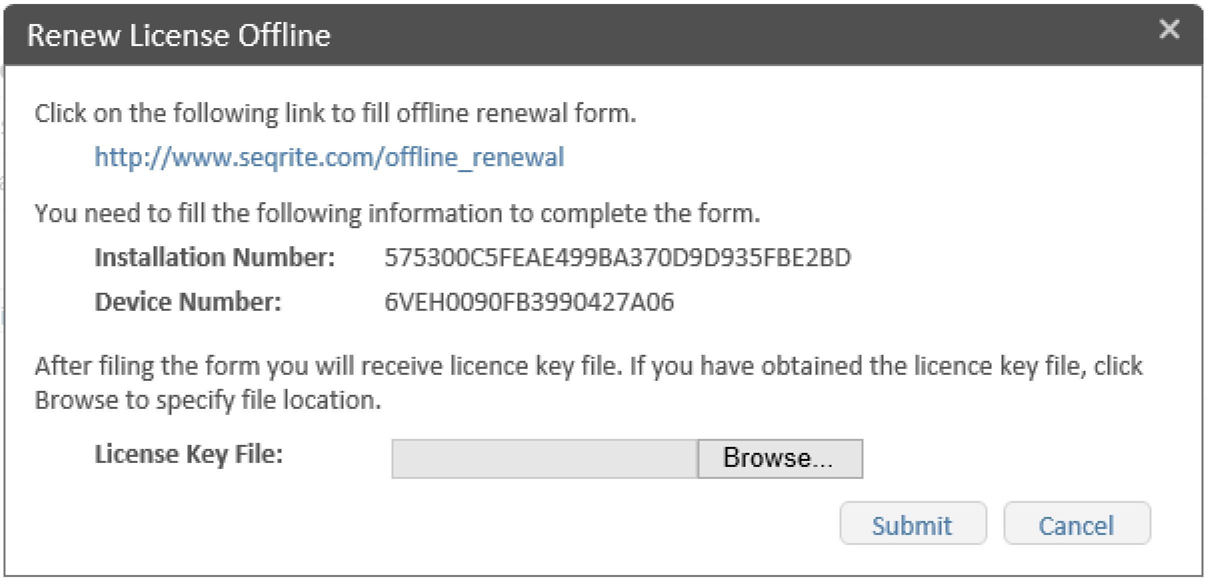
3. The service details section displays the details of the services you have opted for. For e.g. if you have bought the Antispam service, then it will be displayed in this section.
4. If you have renewed the license or added / deleted services or added / deleted users, then these activities will take effect only on clicking the **Update License details** button.
5. 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.



License History Details

Date	Activity	Details
27 April 2015	License Renewed	Duration: 12 Month(s) User(s): 50 Feature(s) Added: AntiSpam, Intrusion Prevention Feature(s) Removed: Virtual Private Network(15), Intrusion Prevention
27 April 2015	License Added	User(s): 35 Feature(s) Added: SMS(5). Feature(s) Removed: AntiSpam
27 April 2015	License Added	User(s): 35 Feature(s) Added: AntiSpam, SMS(27).
27 April 2015	License Added	User(s): 35 Feature(s) Removed: Virtual Private Network(35), AntiSpam
27 April 2015	License Added	User(s): 35 Feature(s) Added: Virtual Private Network(50), AntiSpam, SMS(23).

6. You can 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.



Renew License Offline

Click on the following link to fill offline renewal form.

http://www.seqrite.com/offline_renewal

You need to fill the following information to complete the form.

Installation Number: 575300C5FEAE499BA370D9D935FBE2BD

Device Number: 6VEH0090FB3990427A06

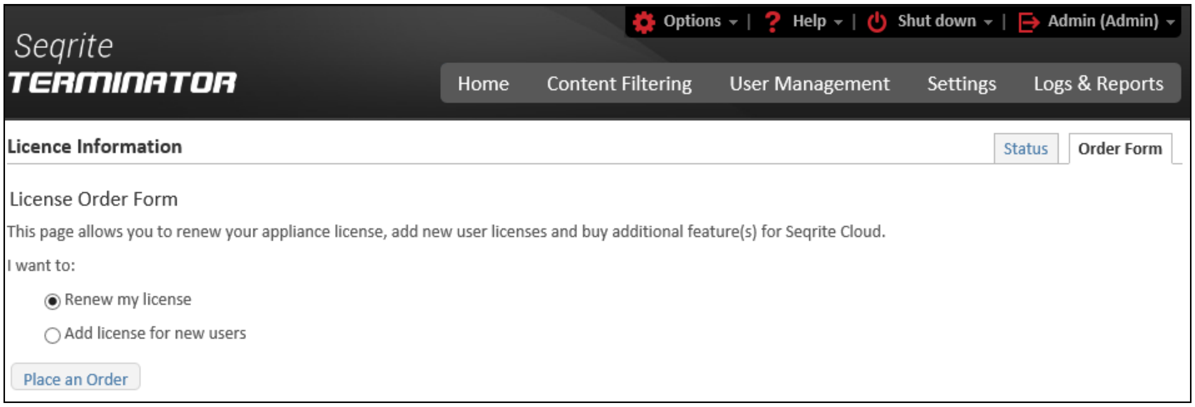
After filing the form you will receive licence key file. If you have obtained the licence key file, click Browse to specify file location.

License Key File: Browse...

Renew License

You can renew the Terminator license as well as add more users for the license using the Order form tab on the License details page. To renew license follow these steps:

1. Log in to Seqrite Terminator **> Help > License details**. The License details page is displayed.
2. Click on the **Order form** tab. The renew license page is displayed.



Licence Information

License Order Form

This page allows you to renew your appliance license, add new user licenses and buy additional feature(s) for Seqrite Cloud.

I want to:

● Renew my license

○ Add license for new users

3. To renew Terminator license, select the **Renew my license** option. To add more users in the license, select the **Add license for new users** option.
4. Click **Place an Order**.

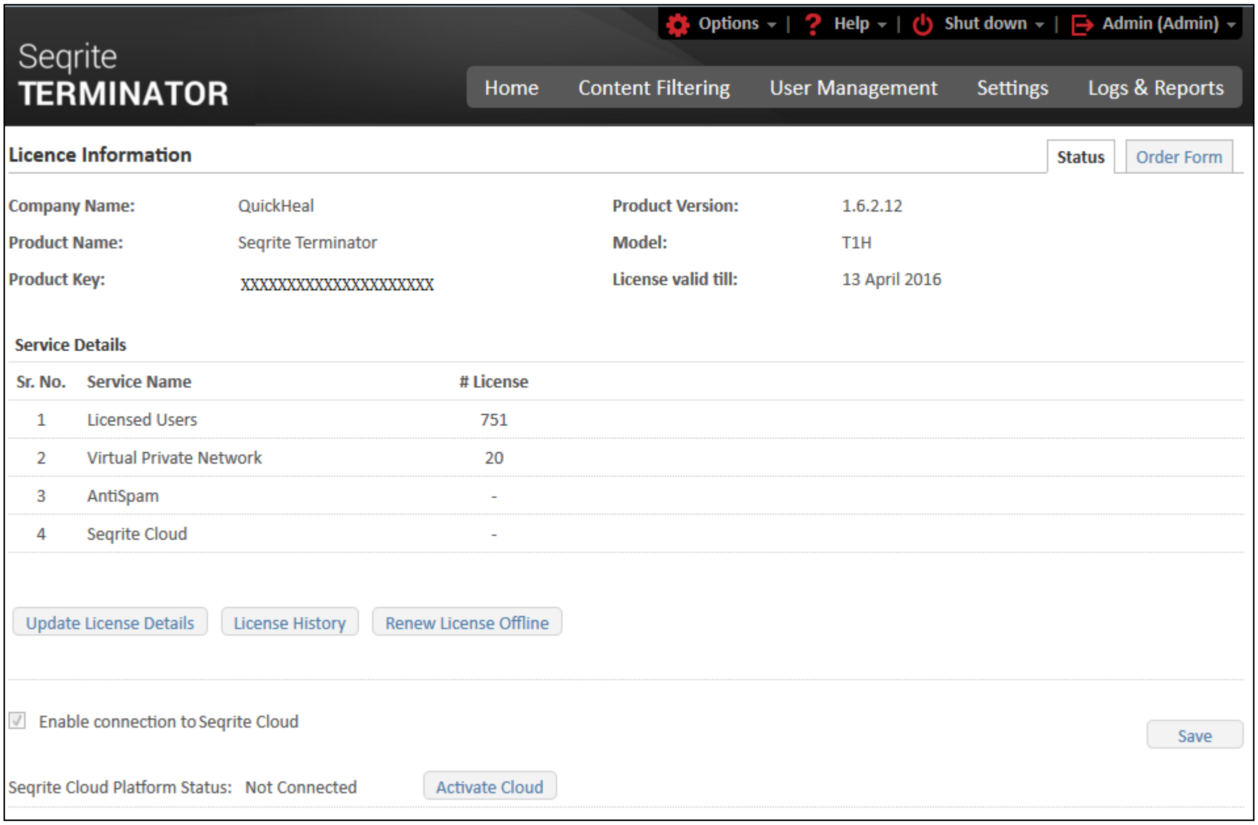
Enabling Seqrite Cloud

Seqrite Cloud is an integrated solution that helps in managing and regulating multiple Terminator deployed at different geographical locations. You can easily connect to the cloud to view the latest security status, configure product policies, receive notifications and rectify critical network events from one single dashboard. It also facilitates policy configuration and backup on the cloud for Terminator.

Note: This feature is paid and optional. You need to contact customer care to enable Cloud feature in your Terminator.

To activate and enable Seqrite cloud service for Terminator follow these steps:

1. Log on to Seqrite Terminator **> Help > License Details**. The License information screen is displayed.



Licence Information

Company Name:	QuickHeal	**Product Version:**	1.6.2.12
Product Name:	Seqrite Terminator	**Model:**	T1H
Product Key:	XXXXXXXXXXXXXXXXXXXXX	**License valid till:**	13 April 2016

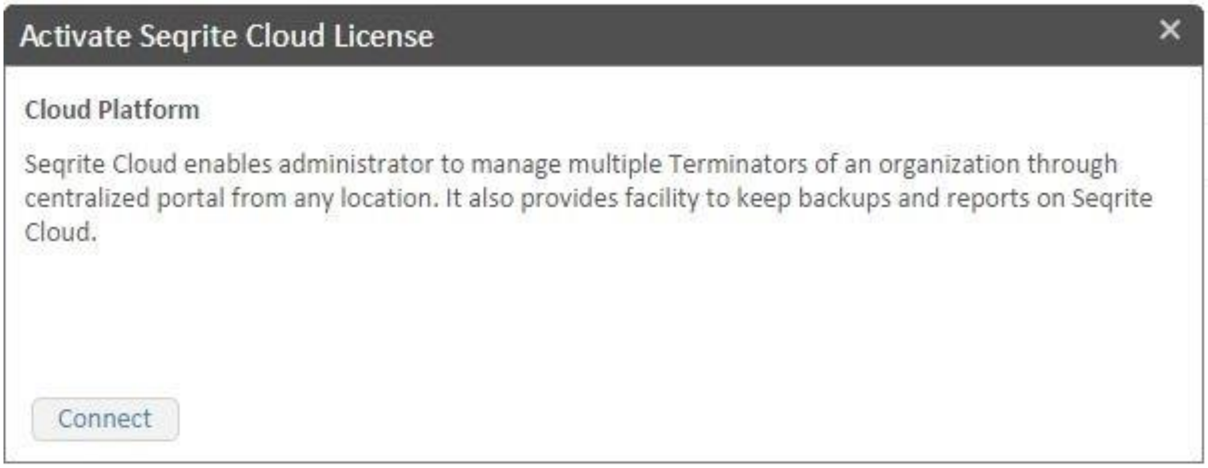
Service Details

Sr. No.	Service Name	# License
1	Licensed Users	751
2	Virtual Private Network	20
3	AntiSpam	-
4	Seqrite Cloud	-

☑ Enable connection to Seqrite Cloud

Seqrite Cloud Platform Status: Not Connected

2. To use the Seqrite Cloud service, you need to first activate it. Click the **Activate cloud** button. The cloud platform information popup is displayed.

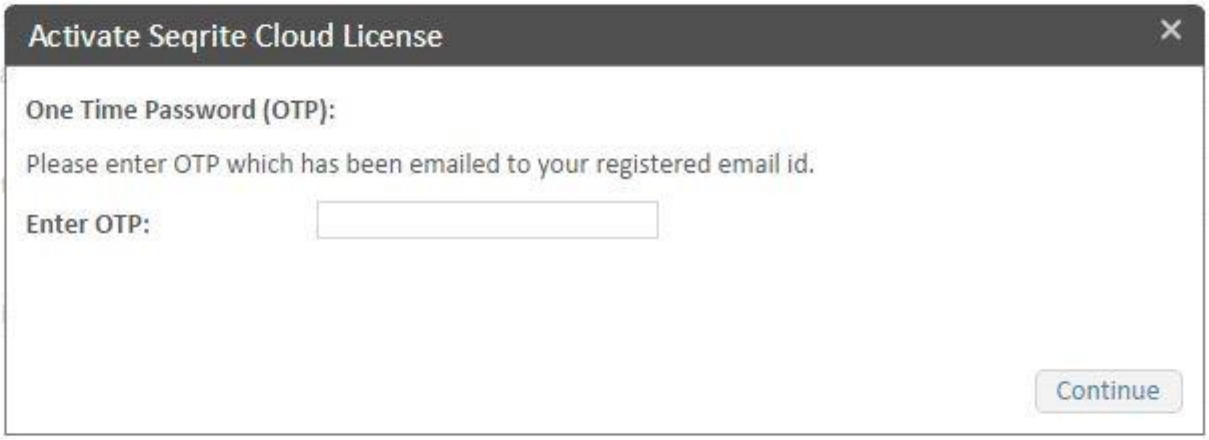


Activate Seqrite Cloud License

Cloud Platform

Seqrite Cloud enables administrator to manage multiple Terminators of an organization through centralized portal from any location. It also provides facility to keep backups and reports on Seqrite Cloud.

3. Click **Connect**, the OPT popup appears and an OTP is sent to your registered email id.



Activate Seqrite Cloud License

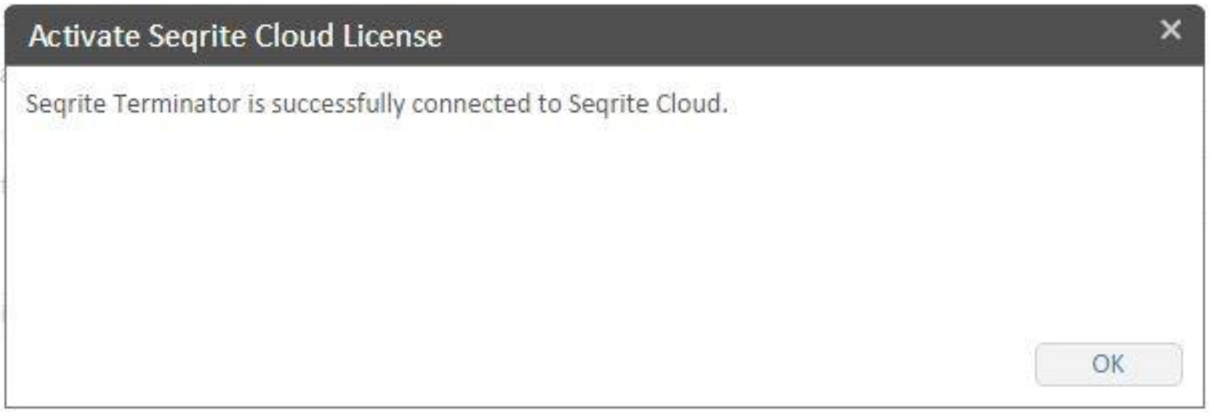
One Time Password (OTP):

Please enter OTP which has been emailed to your registered email id.

Enter OTP:

4. Enter the OTP, which you have received on your registered email id and click **Continue**.

5. On clicking continue, the OPT will be verified. On successful verification the Cloud service will be activated.



Activate Seqrite Cloud License

Seqrite Terminator is successfully connected to Seqrite Cloud.

6. You can enable or disable the Cloud service, using the **“Enable connection to Seqrite Cloud”** field.

Chapter

9

Logs and Reports

Seqrite Terminator 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.

The following types of reports are available on Terminator:

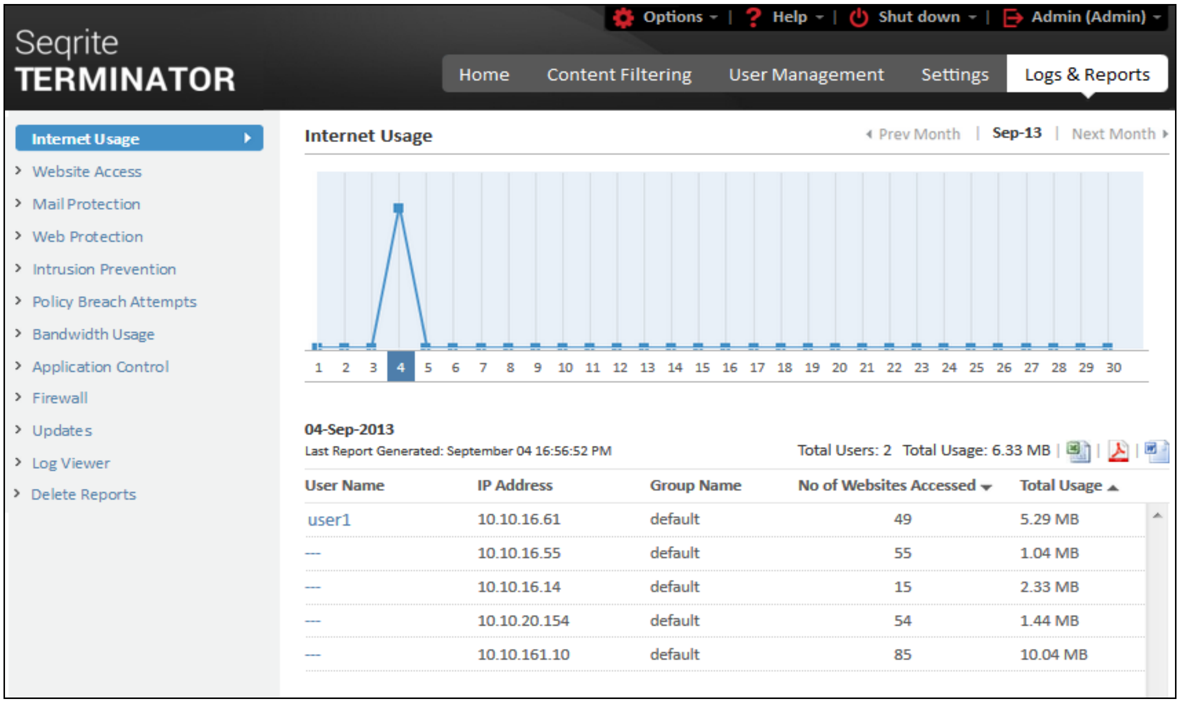
- Internet Usage
- Website Access
- Mail Protection
- Web Protection
- Intrusion Prevention
- Policy Breach Attempts
- Bandwidth Usage
- Application Control
- Firewall Reports
- Updates
- Log Viewer

Internet Usage Report

This report gives data for monthly Internet usage. It provides details such as Total Users, Total Usage, username, IP address of the user, group name to which the user belongs, total number of Web sites accessed by a user, and the total Internet usage. It provides actual bandwidth usage at different time of the day and the different systems using it. This report can be customized to find out the reason for huge traffic generation. The result will allow to take decisions on bandwidth usage and creating company policies to reduce the unwanted or non-work related Internet usage. You can export this report in the MS Excel, PDF and MS Word format.

To view Internet usage logs follow the steps given below:

1. Log on to Seqrite Terminator> **Logs and Reports> Internet Usage**. The following page is displayed.



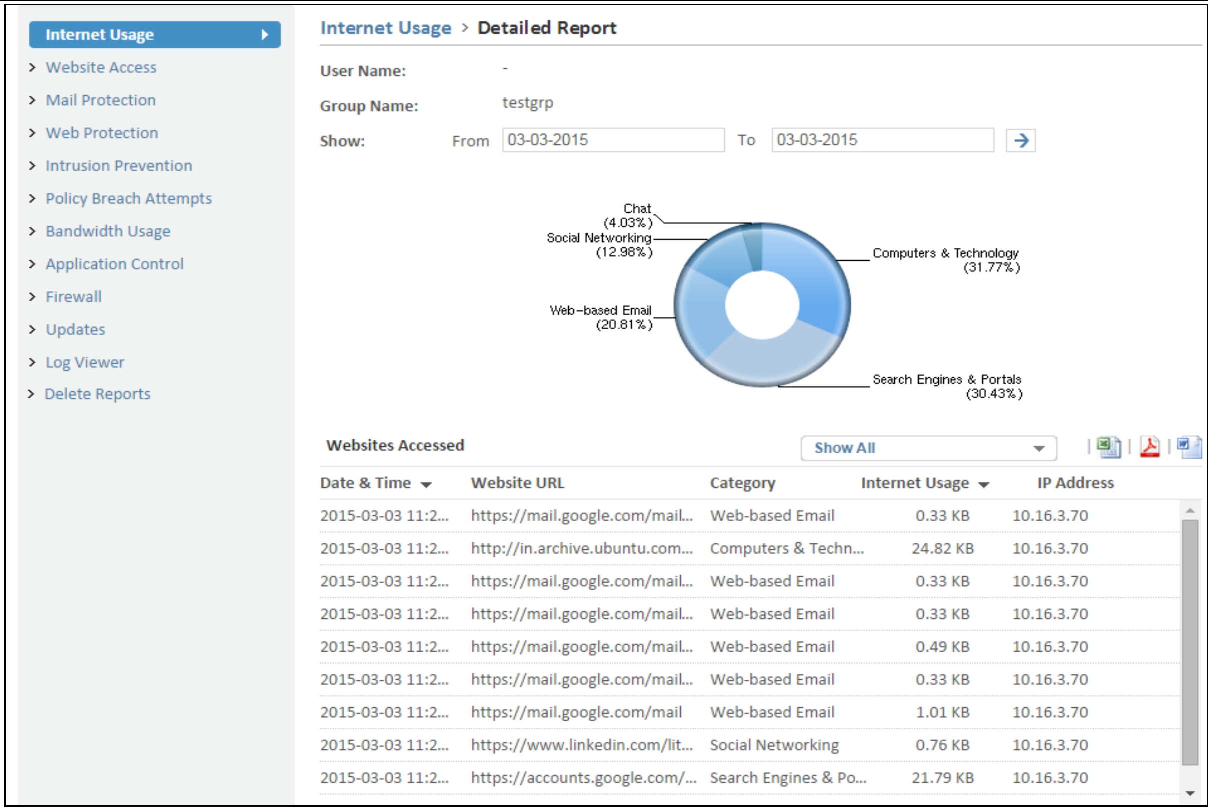
04-Sep-2013

Last Report Generated: September 04 16:56:52 PM

Total Users: 2 Total Usage: 6.33 MB

User Name	IP Address	Group Name	No of Websites Accessed	Total Usage
user1	10.10.16.61	default	49	5.29 MB
---	10.10.16.55	default	55	1.04 MB
---	10.10.16.14	default	15	2.33 MB
---	10.10.20.154	default	54	1.44 MB
---	10.10.161.10	default	85	10.04 MB

2. Click on the User name to view the detailed Internet usage report of the user.



User Name: -

Group Name: testgrp

Show: From 03-03-2015 To 03-03-2015

Websites Accessed

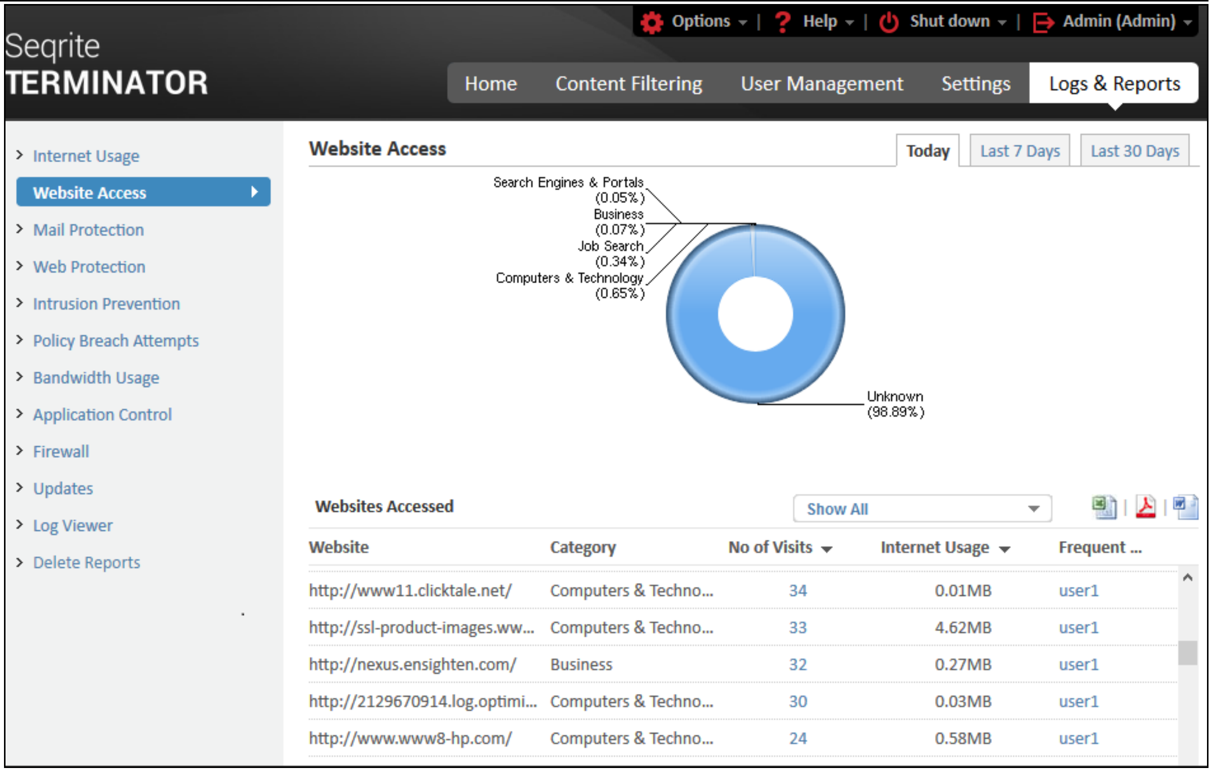
Date & Time	Website URL	Category	Internet Usage	IP Address
2015-03-03 11:2...	https://mail.google.com/mail...	Web-based Email	0.33 KB	10.16.3.70
2015-03-03 11:2...	http://in.archive.ubuntu.com...	Computers & Techn...	24.82 KB	10.16.3.70
2015-03-03 11:2...	https://mail.google.com/mail...	Web-based Email	0.33 KB	10.16.3.70
2015-03-03 11:2...	https://mail.google.com/mail...	Web-based Email	0.33 KB	10.16.3.70
2015-03-03 11:2...	https://mail.google.com/mail...	Web-based Email	0.49 KB	10.16.3.70
2015-03-03 11:2...	https://mail.google.com/mail...	Web-based Email	0.33 KB	10.16.3.70
2015-03-03 11:2...	https://mail.google.com/mail	Web-based Email	1.01 KB	10.16.3.70
2015-03-03 11:2...	https://www.linkedin.com/lit...	Social Networking	0.76 KB	10.16.3.70
2015-03-03 11:2...	https://accounts.google.com/...	Search Engines & Po...	21.79 KB	10.16.3.70

Web site Access Report

This report displays the information about the Web sites accessed by the users for a particular day or last 7 days or last 30 days. It also displays the category-wise Web site access report, the number of visits and lists the frequent visitors to these sites. You can export this report in the MS Excel, PDF and MS Word format.

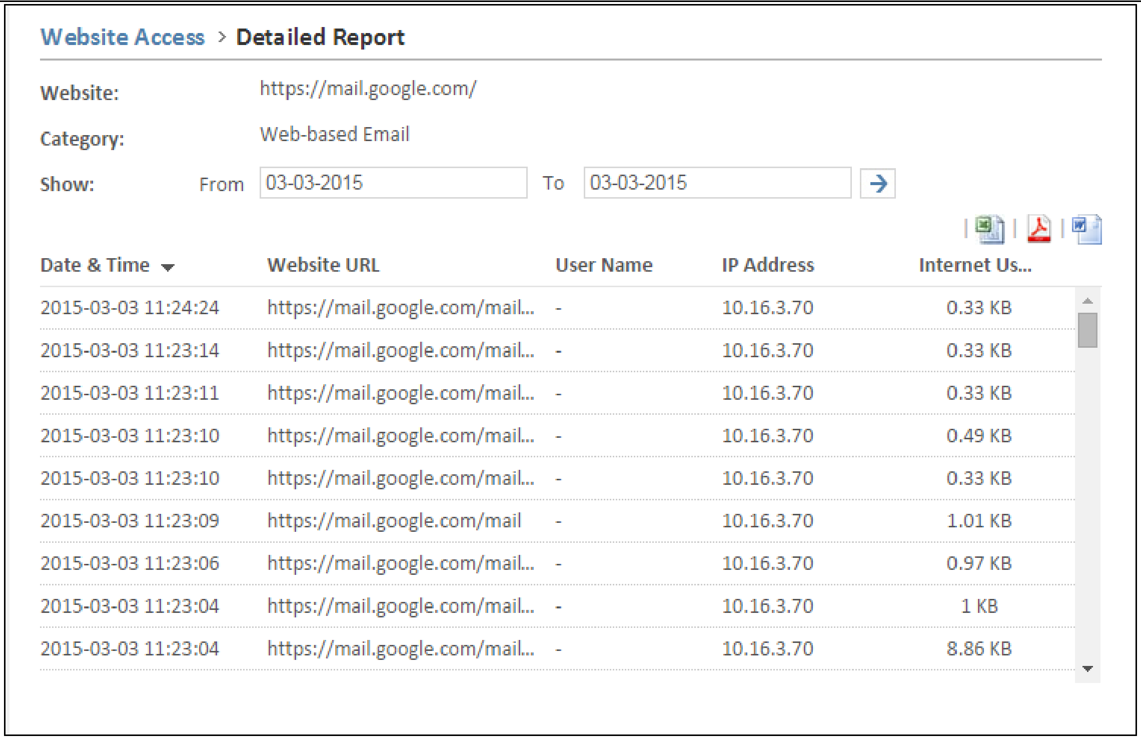
To view Web Site access report follow the steps given below:

1. Log on to Seqrite Terminator > **Logs and Reports> Website Access.** The following page is displayed.



Website	Category	No of Visits	Internet Usage	Frequent ...
http://www11.clicktale.net/	Computers & Techno...	34	0.01MB	user1
http://ssl-product-images.ww...	Computers & Techno...	33	4.62MB	user1
http://nexus.ensighten.com/	Business	32	0.27MB	user1
http://2129670914.log.optimi...	Computers & Techno...	30	0.03MB	user1
http://www.www8-hp.com/	Computers & Techno...	24	0.58MB	user1

2. Click on the **No. of Visits** to view the detailed report of the Web site visits as shown below:



Website Access > Detailed Report

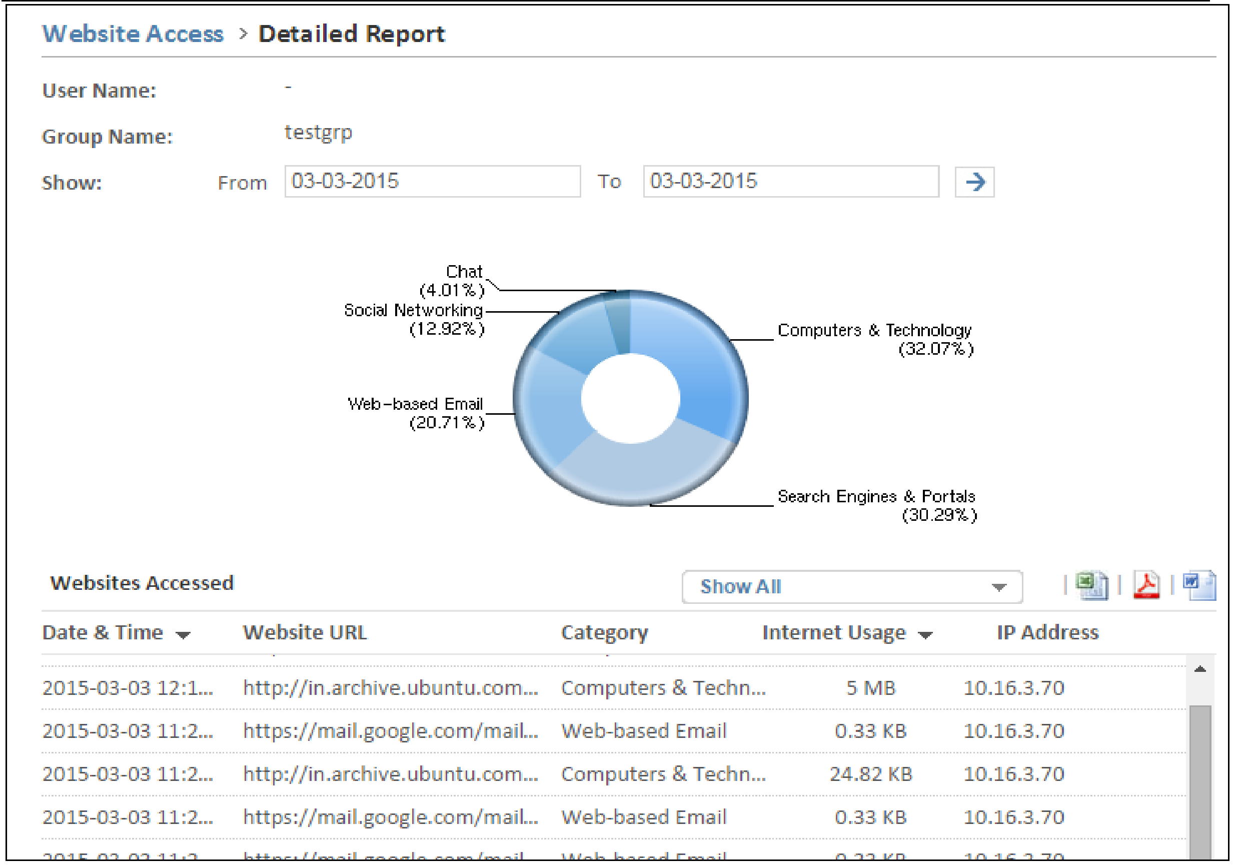
Website: https://mail.google.com/

Category: Web-based Email

Show: From 03-03-2015 To 03-03-2015

Date & Time	Website URL	User Name	IP Address	Internet Us...
2015-03-03 11:24:24	https://mail.google.com/mail...	-	10.16.3.70	0.33 KB
2015-03-03 11:23:14	https://mail.google.com/mail...	-	10.16.3.70	0.33 KB
2015-03-03 11:23:11	https://mail.google.com/mail...	-	10.16.3.70	0.33 KB
2015-03-03 11:23:10	https://mail.google.com/mail...	-	10.16.3.70	0.49 KB
2015-03-03 11:23:10	https://mail.google.com/mail...	-	10.16.3.70	0.33 KB
2015-03-03 11:23:09	https://mail.google.com/mail	-	10.16.3.70	1.01 KB
2015-03-03 11:23:06	https://mail.google.com/mail...	-	10.16.3.70	0.97 KB
2015-03-03 11:23:04	https://mail.google.com/mail...	-	10.16.3.70	1 KB
2015-03-03 11:23:04	https://mail.google.com/mail...	-	10.16.3.70	8.86 KB

3. Click on the **Username** in the **Frequent Visitors** column on the Web site Access report page, to view the detailed report of the user who has frequently accessed the Web site.



Website Access > Detailed Report

User Name: -

Group Name: testgrp

Show: From 03-03-2015 To 03-03-2015

Chat (4.01%)
Social Networking (12.92%)
Web-based Email (20.71%)
Computers & Technology (32.07%)
Search Engines & Portals (30.29%)

Websites Accessed

Show All

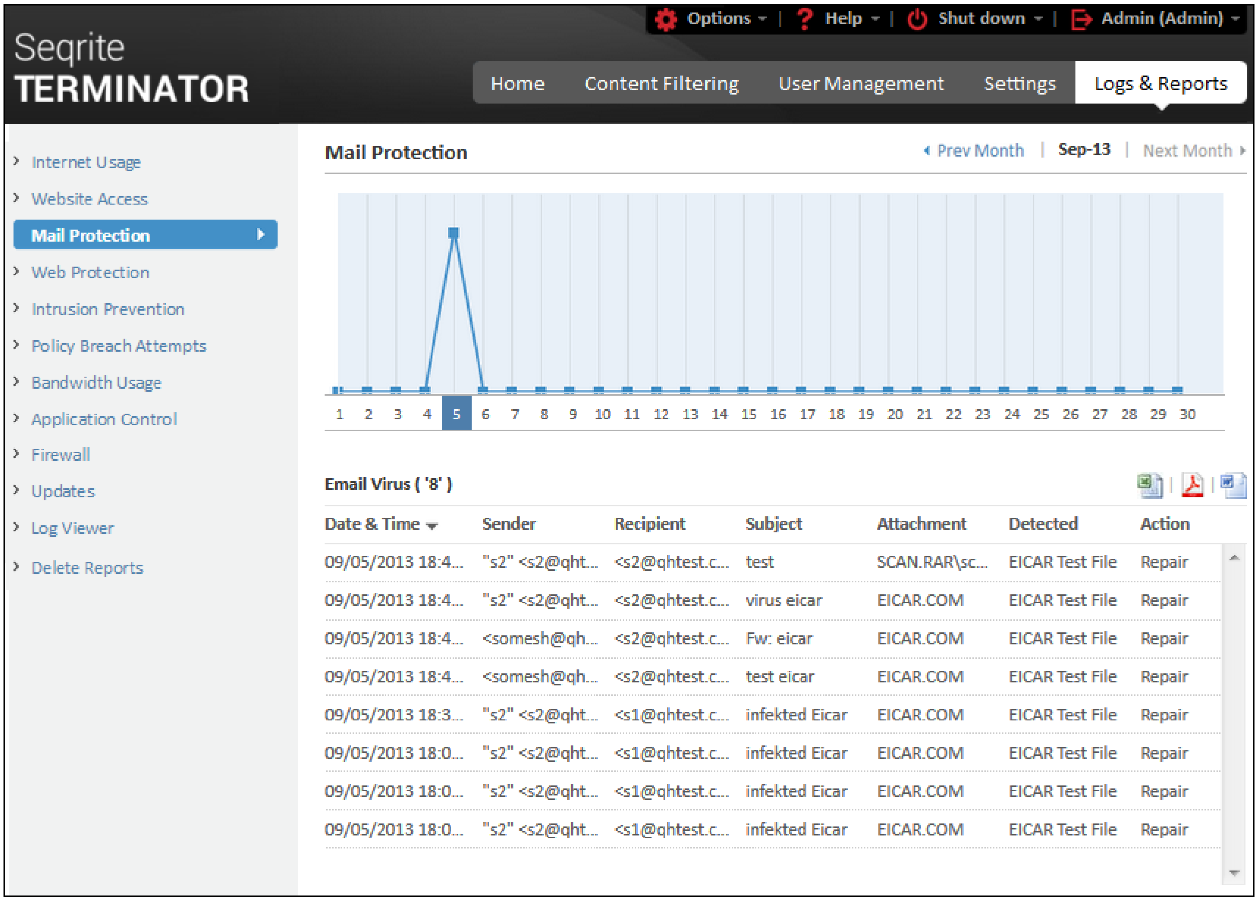
Date & Time	Website URL	Category	Internet Usage	IP Address
2015-03-03 12:1...	http://in.archive.ubuntu.com...	Computers & Techn...	5 MB	10.16.3.70
2015-03-03 11:2...	https://mail.google.com/mail...	Web-based Email	0.33 KB	10.16.3.70
2015-03-03 11:2...	http://in.archive.ubuntu.com...	Computers & Techn...	24.82 KB	10.16.3.70
2015-03-03 11:2...	https://mail.google.com/mail...	Web-based Email	0.33 KB	10.16.3.70
2015-03-03 11:2...	https://mail.google.com/mail...	Web-based Email	0.33 KB	10.16.3.70

Mail Protection Report

Seqrite Terminator 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.

To view mail protection reports follow the steps given below:

1. Log on to Seqrite Terminator **> Logs and Reports > Mail Protection.** The following page is displayed.



Email Virus ('8')

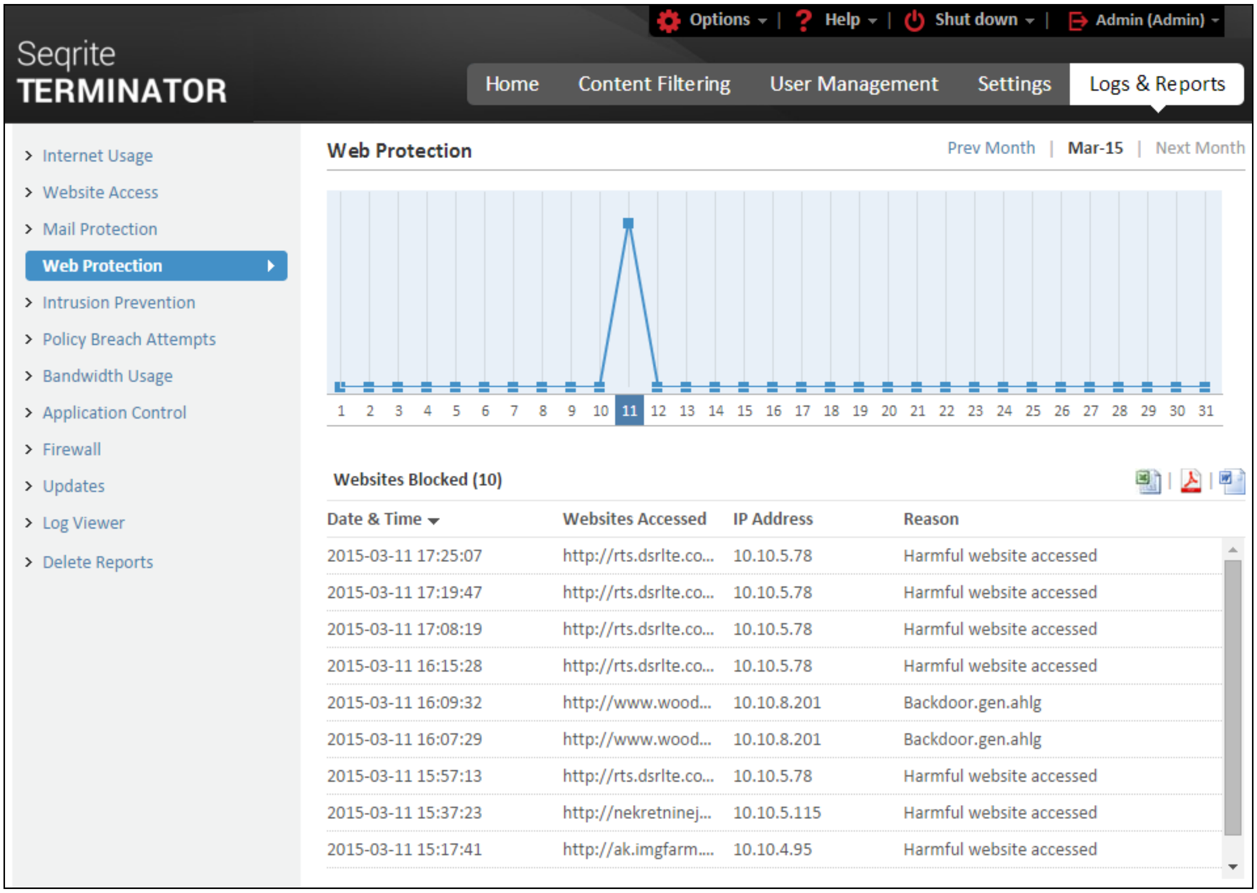
Date & Time	Sender	Recipient	Subject	Attachment	Detected	Action
09/05/2013 18:4...	"s2" <s2@qht...	<s2@qhtest.c...	test	SCAN.RAR\sc...	EICAR Test File	Repair
09/05/2013 18:4...	"s2" <s2@qht...	<s2@qhtest.c...	virus eicar	EICAR.COM	EICAR Test File	Repair
09/05/2013 18:4...	<somesh@qh...	<s2@qhtest.c...	Fw: eicar	EICAR.COM	EICAR Test File	Repair
09/05/2013 18:4...	<somesh@qh...	<s2@qhtest.c...	test eicar	EICAR.COM	EICAR Test File	Repair
09/05/2013 18:3...	"s2" <s2@qht...	<s1@qhtest.c...	infekted Eicar	EICAR.COM	EICAR Test File	Repair
09/05/2013 18:0...	"s2" <s2@qht...	<s1@qhtest.c...	infekted Eicar	EICAR.COM	EICAR Test File	Repair
09/05/2013 18:0...	"s2" <s2@qht...	<s1@qhtest.c...	infekted Eicar	EICAR.COM	EICAR Test File	Repair
09/05/2013 18:0...	"s2" <s2@qht...	<s1@qhtest.c...	infekted Eicar	EICAR.COM	EICAR Test File	Repair

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.

To view web protection reports follow the steps given below:

1. Log on to Seqrite Terminator> **Logs and Reports> Web Protection.** The following page is displayed. The following page is displayed.



Web Protection

Websites Blocked (10)

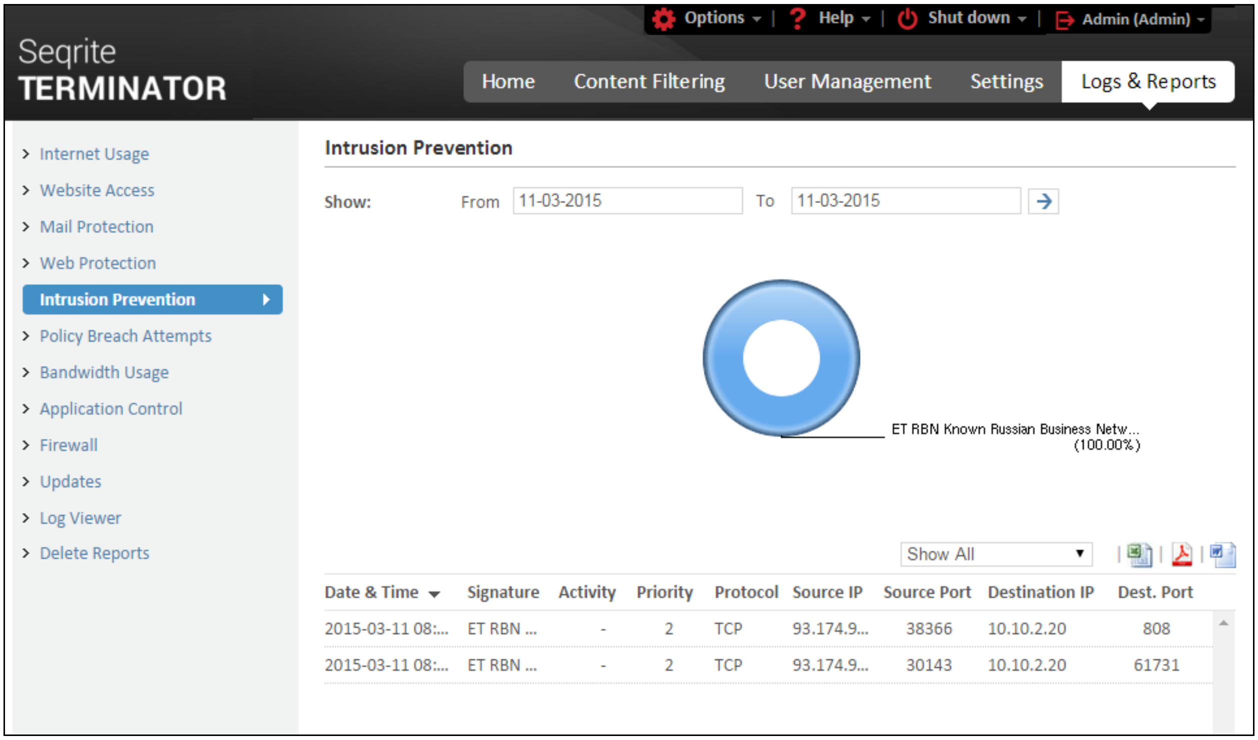
Date & Time	Websites Accessed	IP Address	Reason
2015-03-11 17:25:07	http://rts.dsrlte.co...	10.10.5.78	Harmful website accessed
2015-03-11 17:19:47	http://rts.dsrlte.co...	10.10.5.78	Harmful website accessed
2015-03-11 17:08:19	http://rts.dsrlte.co...	10.10.5.78	Harmful website accessed
2015-03-11 16:15:28	http://rts.dsrlte.co...	10.10.5.78	Harmful website accessed
2015-03-11 16:09:32	http://www.wood...	10.10.8.201	Backdoor.gen.ahlg
2015-03-11 16:07:29	http://www.wood...	10.10.8.201	Backdoor.gen.ahlg
2015-03-11 15:57:13	http://rts.dsrlte.co...	10.10.5.78	Harmful website accessed
2015-03-11 15:37:23	http://nekretninej...	10.10.5.115	Harmful website accessed
2015-03-11 15:17:41	http://ak.imgfarm....	10.10.4.95	Harmful website accessed

Intrusion Prevention Report

The Intrusion Prevention report provides information about intrusions that were prevented by the Terminator. 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.

To view policy breach reports follow the steps given below:

1. Log on to Seqrite Terminator **> Logs and Reports > Intrusion Prevention.** The following page is displayed.



Intrusion Prevention

Show: From 11-03-2015 To 11-03-2015

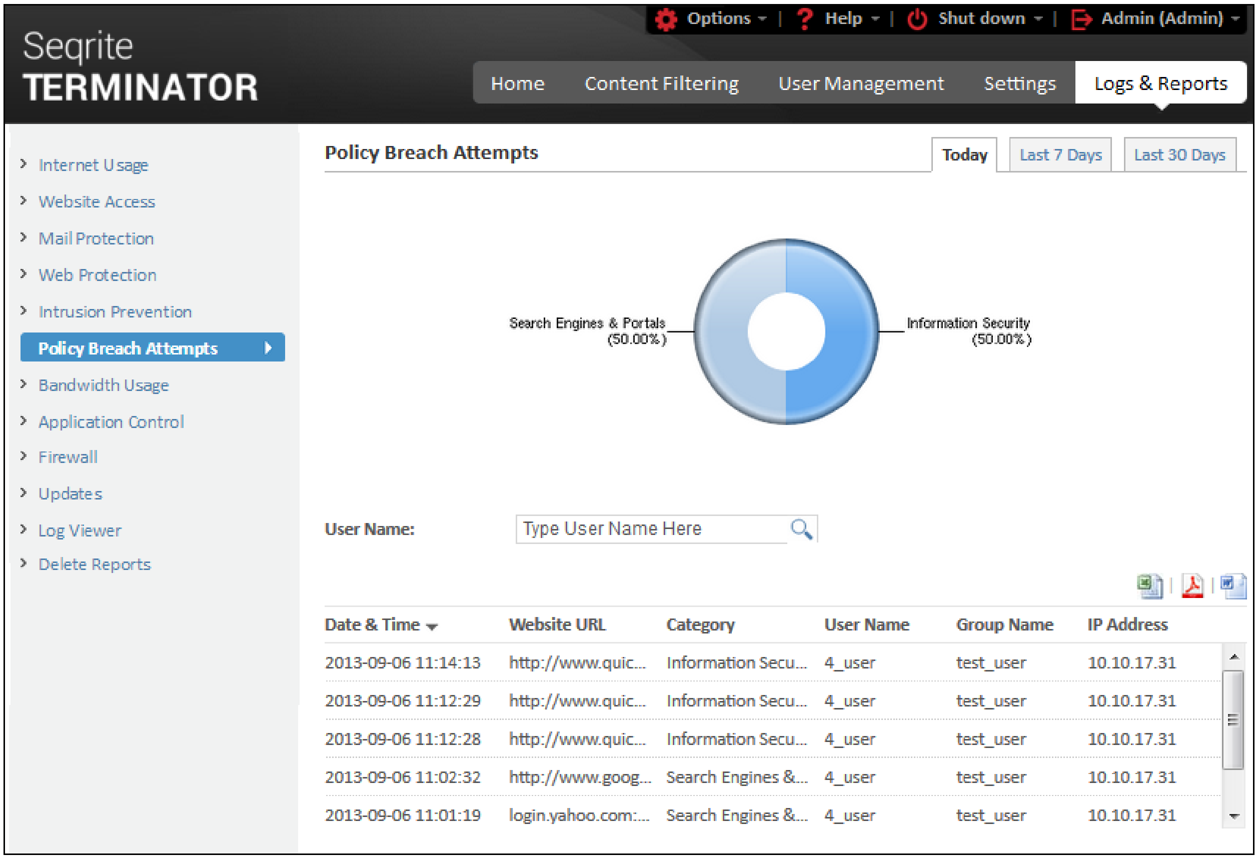
Date & Time	Signature	Activity	Priority	Protocol	Source IP	Source Port	Destination IP	Dest. Port
2015-03-11 08:...	ET RBN ...	-	2	TCP	93.174.9...	38366	10.10.2.20	808
2015-03-11 08:...	ET RBN ...	-	2	TCP	93.174.9...	30143	10.10.2.20	61731

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.

To View policy breach reports follow the steps given below:

1. Log on to Seqrite Terminator> **Logs and Reports> Policy Breach Attempts.** The following page is displayed.



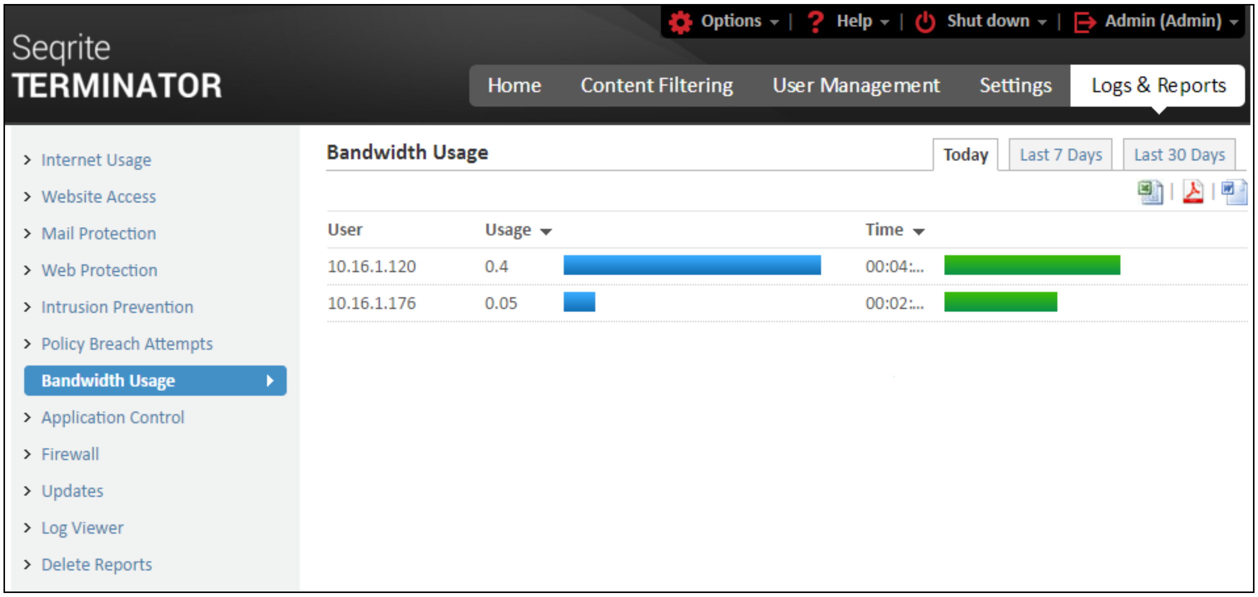
Date & Time	Website URL	Category	User Name	Group Name	IP Address
2013-09-06 11:14:13	http://www.quic...	Information Secu...	4_user	test_user	10.10.17.31
2013-09-06 11:12:29	http://www.quic...	Information Secu...	4_user	test_user	10.10.17.31
2013-09-06 11:12:28	http://www.quic...	Information Secu...	4_user	test_user	10.10.17.31
2013-09-06 11:02:32	http://www.goog...	Search Engines &...	4_user	test_user	10.10.17.31
2013-09-06 11:01:19	login.yahoo.com:...	Search Engines &...	4_user	test_user	10.10.17.31

Bandwidth Usage Report

The Bandwidth Usage report provides the information about the Internet bandwidth usage. It provides information on the bandwidth used by the user in certain time. This report is available for current day, Last 7 days and last 30 days. This report can be used to formulate policies for bandwidth usage.

To view the bandwidth usage reports, follow the steps given below:

1. Log on to Seqrite Terminator> **Logs and Reports> Bandwidth Usage.** The following page is displayed.



Bandwidth Usage

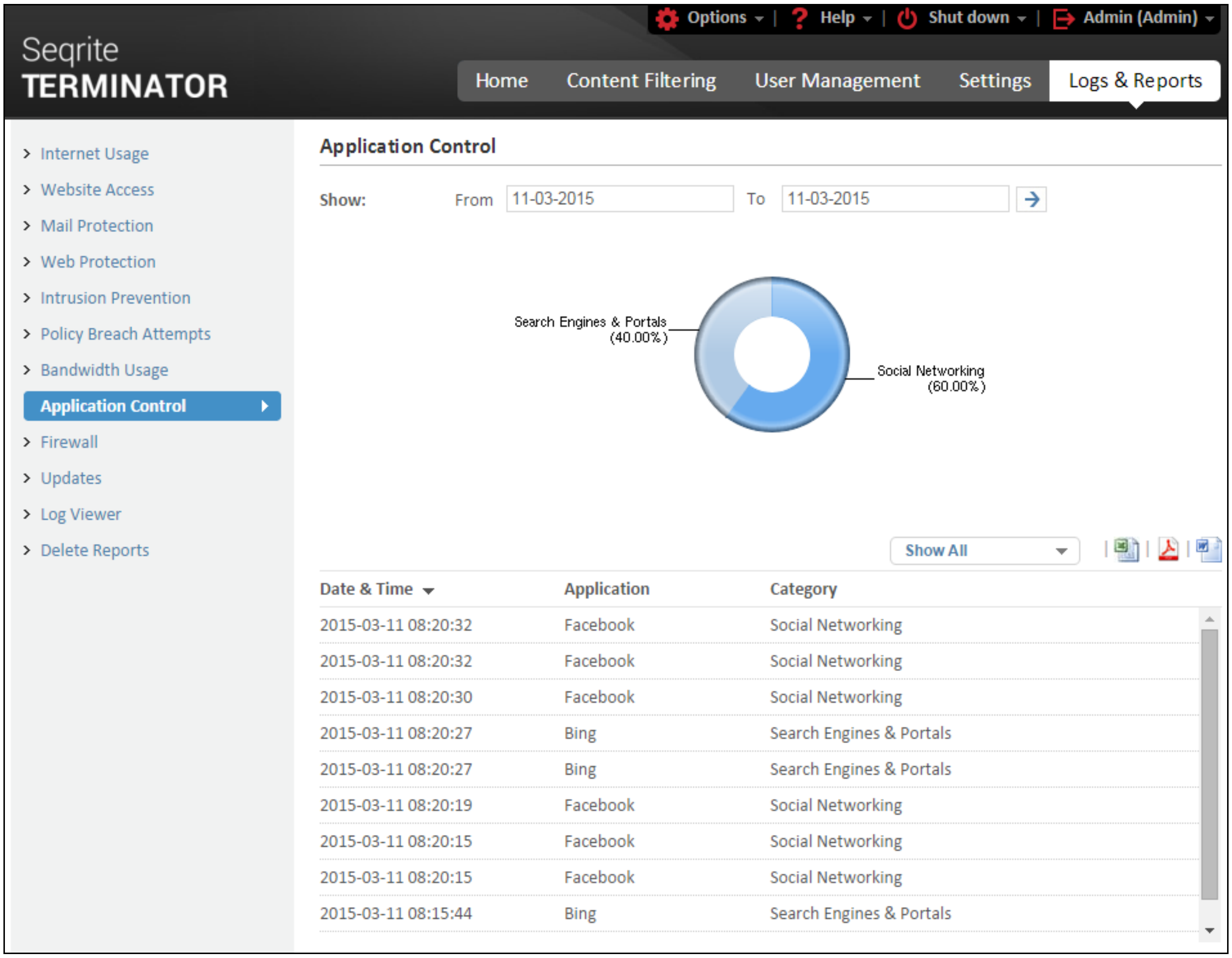
User	Usage	Time
10.16.1.120	0.4	00:04:...
10.16.1.176	0.05	00:02:...

Application Control Report

The application control report provides information about the applications that are prevented by the Terminator. It details timestamp of prevented application, application name and associated category.

To view the application control reports follow the steps given below:

1. Log on to Seqrite Terminator> **Logs and Reports> Application Control.** The following page is displayed.



Application Control

Show: From 11-03-2015 To 11-03-2015

Date & Time	Application	Category
2015-03-11 08:20:32	Facebook	Social Networking
2015-03-11 08:20:32	Facebook	Social Networking
2015-03-11 08:20:30	Facebook	Social Networking
2015-03-11 08:20:27	Bing	Search Engines & Portals
2015-03-11 08:20:27	Bing	Search Engines & Portals
2015-03-11 08:20:19	Facebook	Social Networking
2015-03-11 08:20:15	Facebook	Social Networking
2015-03-11 08:20:15	Facebook	Social Networking
2015-03-11 08:15:44	Bing	Search Engines & Portals

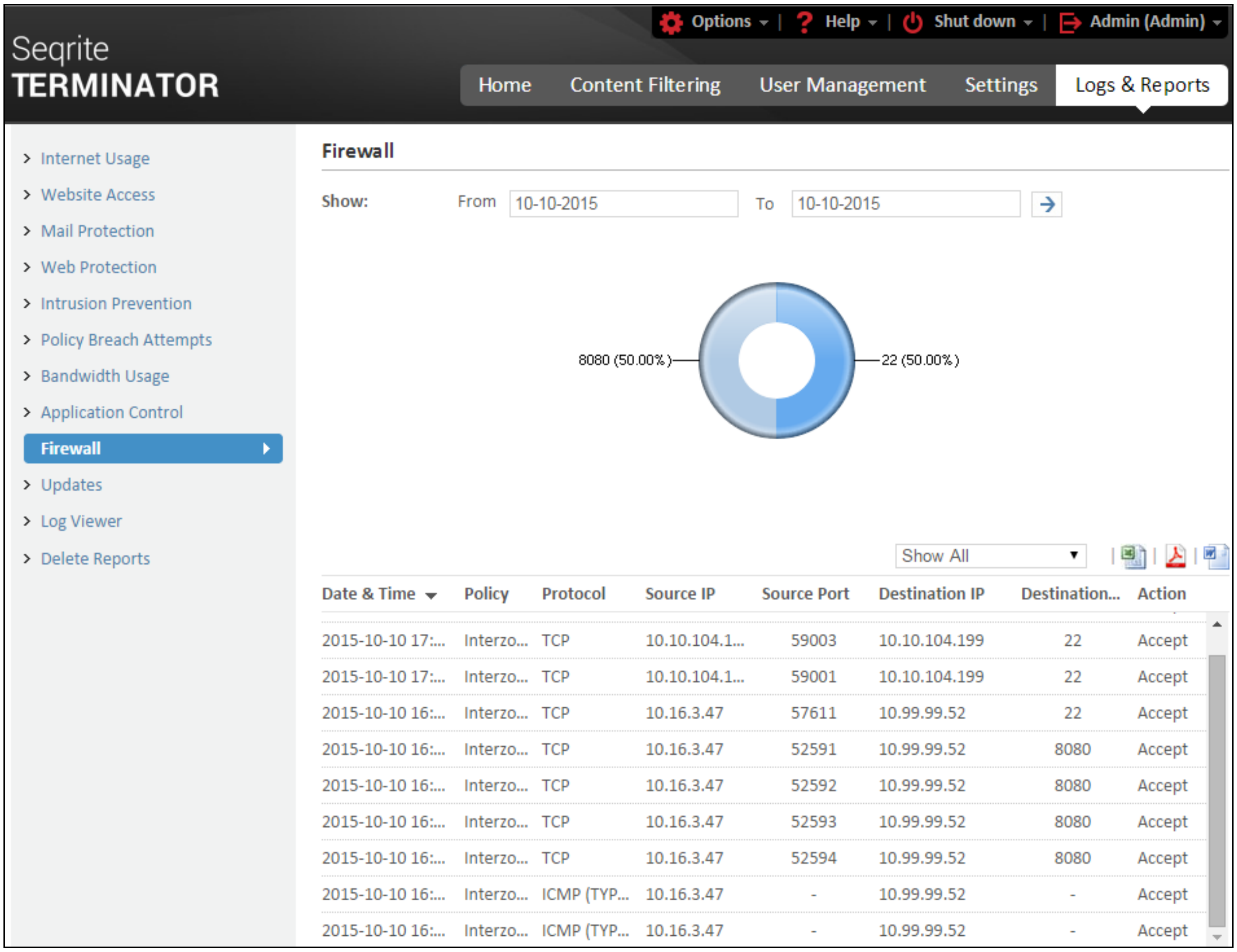
Firewall Reports

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 Terminator. You can also download the report in XLS, Word and PDF format.

To view Firewall reports follow the steps given below:

1. Log on to Seqrite Terminator> **Logs and Reports> Firewall.** The following page is displayed.



Show: From 10-10-2015 To 10-10-2015

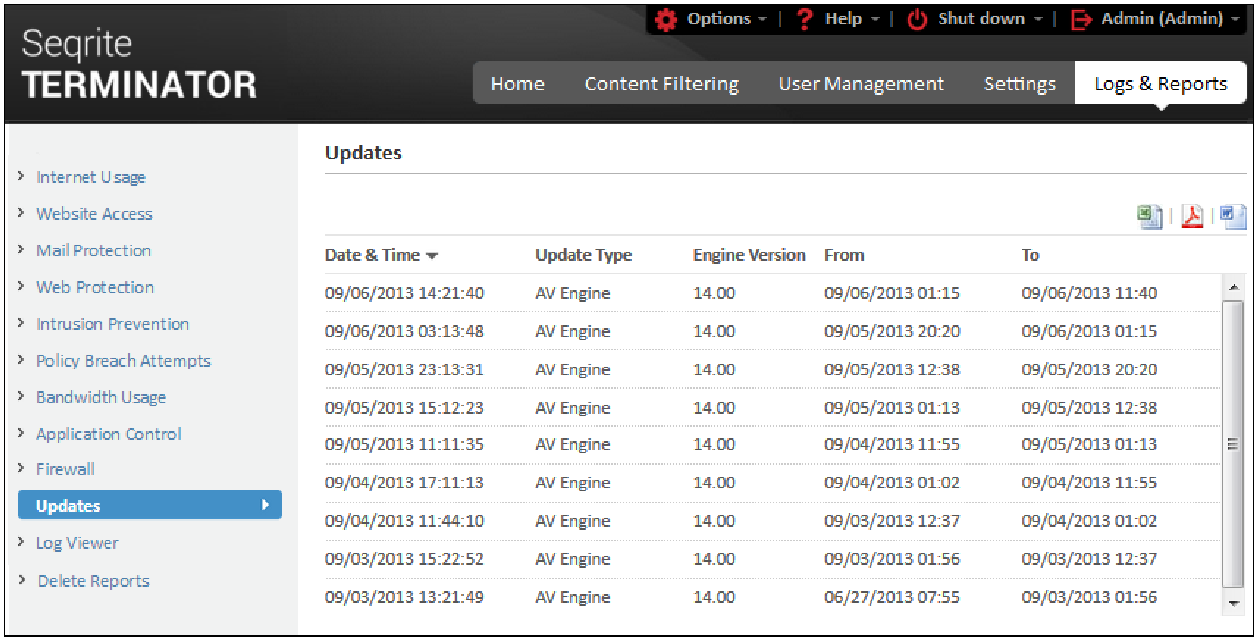
Date & Time	Policy	Protocol	Source IP	Source Port	Destination IP	Destination...	Action
2015-10-10 17:...	Interzo...	TCP	10.10.104.1...	59003	10.10.104.199	22	Accept
2015-10-10 17:...	Interzo...	TCP	10.10.104.1...	59001	10.10.104.199	22	Accept
2015-10-10 16:...	Interzo...	TCP	10.16.3.47	57611	10.99.99.52	22	Accept
2015-10-10 16:...	Interzo...	TCP	10.16.3.47	52591	10.99.99.52	8080	Accept
2015-10-10 16:...	Interzo...	TCP	10.16.3.47	52592	10.99.99.52	8080	Accept
2015-10-10 16:...	Interzo...	TCP	10.16.3.47	52593	10.99.99.52	8080	Accept
2015-10-10 16:...	Interzo...	TCP	10.16.3.47	52594	10.99.99.52	8080	Accept
2015-10-10 16:...	Interzo...	ICMP (TYP...	10.16.3.47	-	10.99.99.52	-	Accept
2015-10-10 16:...	Interzo...	ICMP (TYP...	10.16.3.47	-	10.99.99.52	-	Accept

Updates

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.

To view Update reports follow the steps given below:

2. Log on to Seqrite Terminator> **Logs and Reports> Updates.** The following page is displayed.



Updates

Date & Time	Update Type	Engine Version	From	To
09/06/2013 14:21:40	AV Engine	14.00	09/06/2013 01:15	09/06/2013 11:40
09/06/2013 03:13:48	AV Engine	14.00	09/05/2013 20:20	09/06/2013 01:15
09/05/2013 23:13:31	AV Engine	14.00	09/05/2013 12:38	09/05/2013 20:20
09/05/2013 15:12:23	AV Engine	14.00	09/05/2013 01:13	09/05/2013 12:38
09/05/2013 11:11:35	AV Engine	14.00	09/04/2013 11:55	09/05/2013 01:13
09/04/2013 17:11:13	AV Engine	14.00	09/04/2013 01:02	09/04/2013 11:55
09/04/2013 11:44:10	AV Engine	14.00	09/03/2013 12:37	09/04/2013 01:02
09/03/2013 15:22:52	AV Engine	14.00	09/03/2013 01:56	09/03/2013 12:37
09/03/2013 13:21:49	AV Engine	14.00	06/27/2013 07:55	09/03/2013 01:56

Log Viewer

Use the log viewer on the Seqrite Terminator 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 two tabbed groups, Todays Logs (current logs) and Archived Logs.

Today's logs tab

Displays system logs for the current day. These logs include messages generated by Terminator, user activities, admin activities, updates, logs related to VPN, DHCP and interfaces. You can download or select and delete the logs as required.

Archived Logs tab

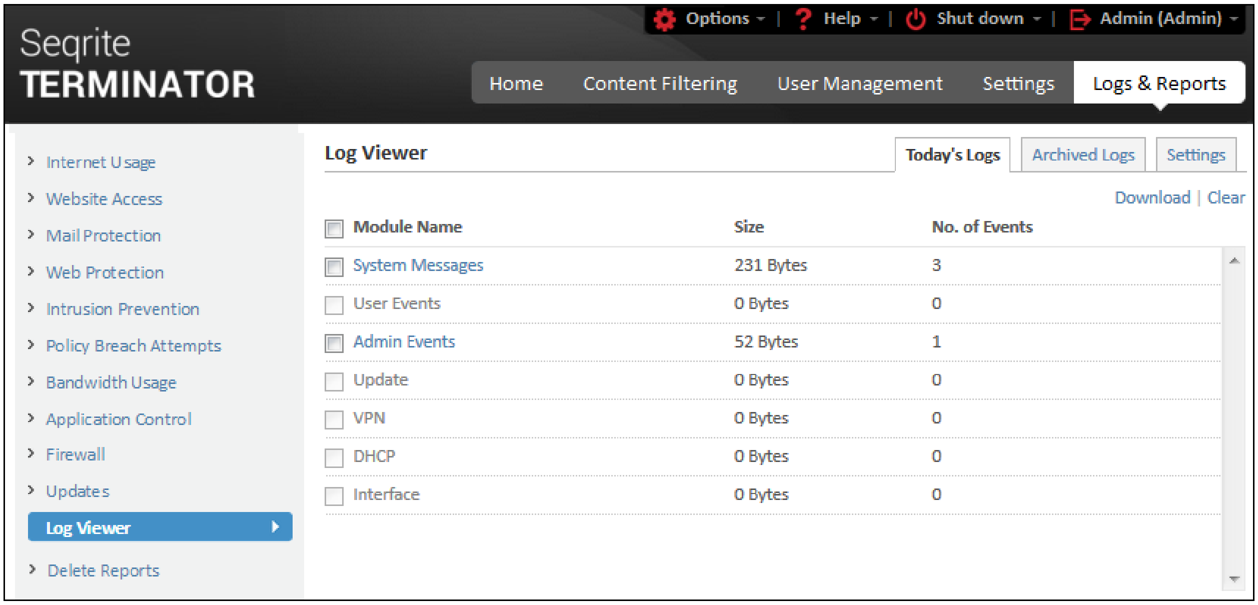
This section displays module-wise log of event or service. You can also browse through the logs month-wise. You can download or delete the logs as required.

Settings tab – Purging (Deleting) old log files

The Settings tab on the Log viewer page 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.

Viewing a today's log

1. Log on to the Terminator> **Logs and Reports > Log Viewer**.

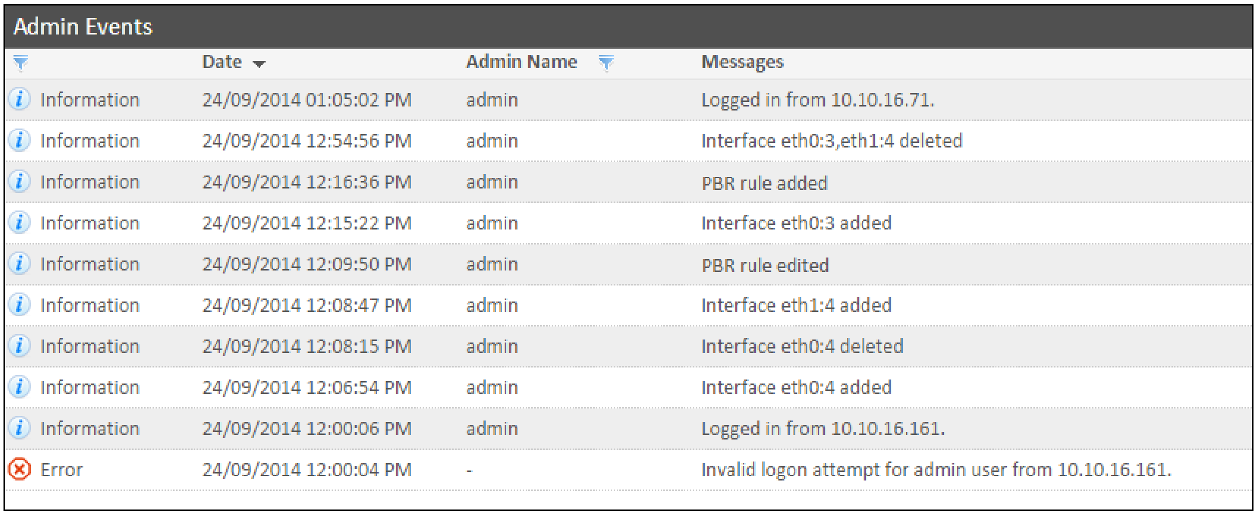


Log Viewer

☐ Module Name	Size	No. of Events
☐ System Messages	231 Bytes	3
☐ User Events	0 Bytes	0
☐ Admin Events	52 Bytes	1
☐ Update	0 Bytes	0
☐ VPN	0 Bytes	0
☐ DHCP	0 Bytes	0
☐ Interface	0 Bytes	0

2. The Todays Log page is displayed that contains various logs of Terminator subsystems along with the module name, log size and log count.

3. To view the current day's logs for a module, click the module name and a popup window displaying the detailed system logs for the current day appears.



Admin Events

	Date	Admin Name	Messages
Information	24/09/2014 01:05:02 PM	admin	Logged in from 10.10.16.71.
Information	24/09/2014 12:54:56 PM	admin	Interface eth0:3,eth1:4 deleted
Information	24/09/2014 12:16:36 PM	admin	PBR rule added
Information	24/09/2014 12:15:22 PM	admin	Interface eth0:3 added
Information	24/09/2014 12:09:50 PM	admin	PBR rule edited
Information	24/09/2014 12:08:47 PM	admin	Interface eth1:4 added
Information	24/09/2014 12:08:15 PM	admin	Interface eth0:4 deleted
Information	24/09/2014 12:06:54 PM	admin	Interface eth0:4 added
Information	24/09/2014 12:00:06 PM	admin	Logged in from 10.10.16.161.
Error	24/09/2014 12:00:04 PM	-	Invalid logon attempt for admin user from 10.10.16.161.

The following details are covered in the detailed log:

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.

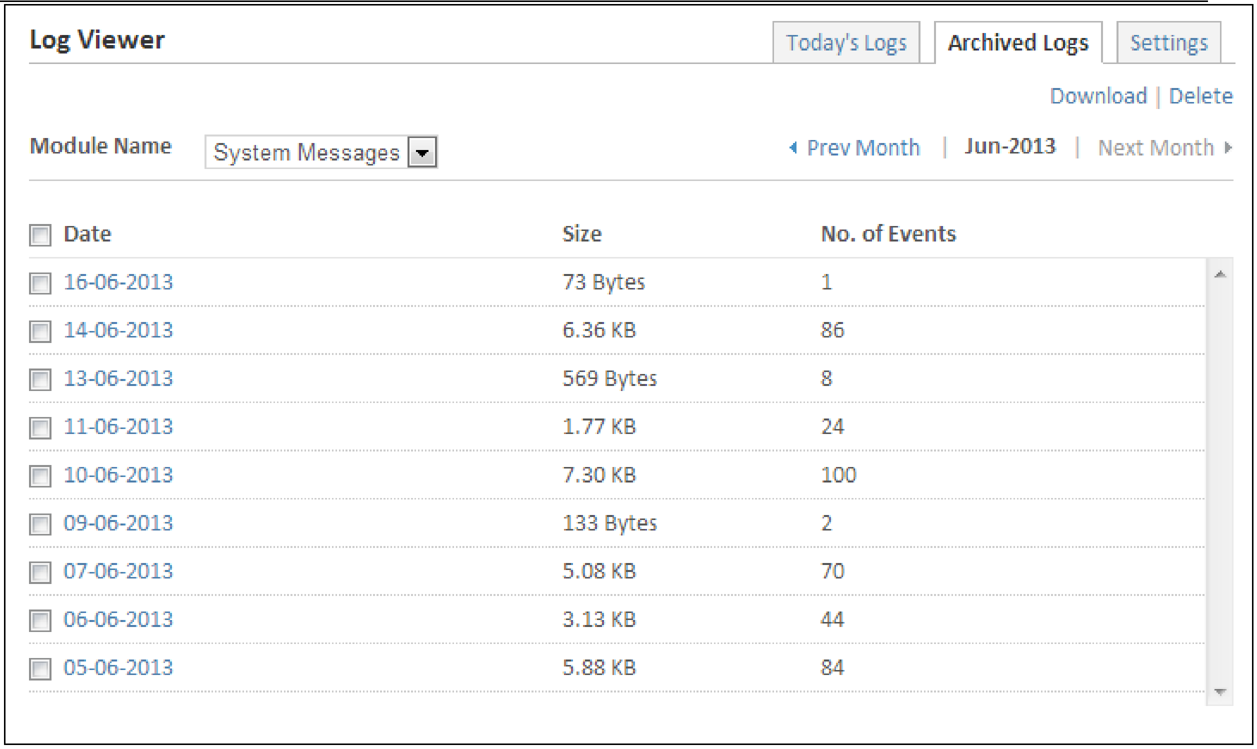
d. The third column shows the name of the Admin.

e. The last column displays the actual log message.

Viewing Archived Logs

To view archived logs follow the steps given below:

1. Log on to the Terminator**> Logs and Reports > Log Viewer> Archived Logs.** The archived log page is displayed as shown below:



Module Name: System Messages

□ Date	Size	No. of Events
□ 16-06-2013	73 Bytes	1
□ 14-06-2013	6.36 KB	86
□ 13-06-2013	569 Bytes	8
□ 11-06-2013	1.77 KB	24
□ 10-06-2013	7.30 KB	100
□ 09-06-2013	133 Bytes	2
□ 07-06-2013	5.08 KB	70
□ 06-06-2013	3.13 KB	44
□ 05-06-2013	5.88 KB	84

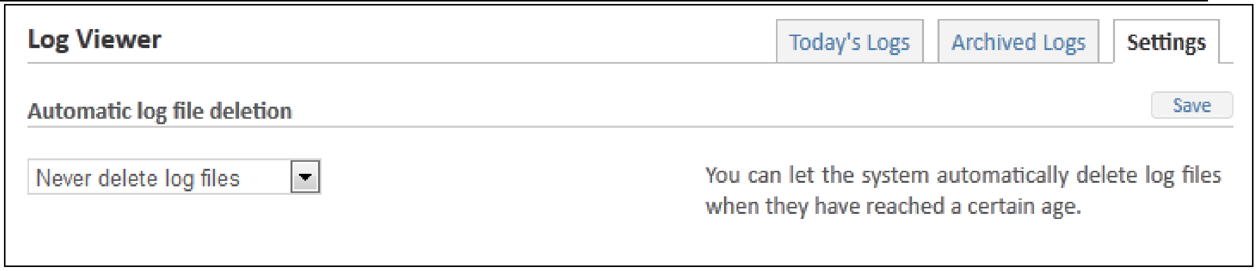
2. Select the **Module Name** from the drop-down. The logs for the selected module is displayed for the current month.

3. You can also view the logs for previous and next month.

Automatically Deleting Log File

To set Terminator to delete old log file automatically, follow the steps given below:

1. Log on to the Terminator**> Logs and Reports > Log Viewer>Settings**. The following page is displayed.



Automatic log file deletion

Never delete log files

You can let the system automatically delete log files when they have reached a certain age.

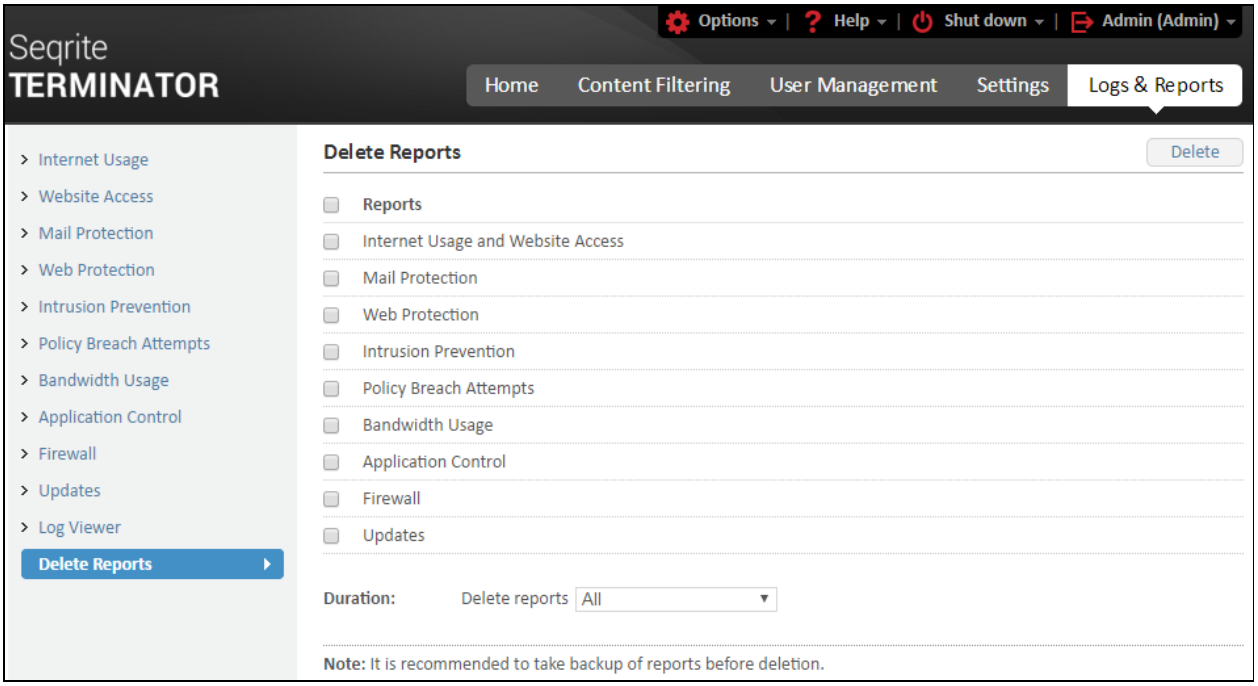
2. Select the duration from the drop-down. Click **Save** when you want to delete the logs. The Terminator will automatically delete log files when they have reached the specified age.

Delete Report

The **Delete Report** section allows you to delete reports for multiple modules for a specified duration.

To delete reports follow these steps:

1. Log on to the Terminator **> Logs and Reports > Delete Reports**.



Delete Reports

- □ **Reports**
- □ Internet Usage and Website Access
- □ Mail Protection
- □ Web Protection
- □ Intrusion Prevention
- □ Policy Breach Attempts
- □ Bandwidth Usage
- □ Application Control
- □ Firewall
- □ Updates

Duration: Delete reports All

Note: It is recommended to take backup of reports before deletion.

2. Select the module(s) for which you want to delete reports.

3. Select the **Duration**. This can be as follow:

   a. All: Allows you to delete all the reports of the selected module(s).IF

   b. All except today's: Allows to delete all reports of the selected module(s) except the report of the current date.

   c. Till: Allows to delete reports of the selected module(s) till the specified date.

   For example:

   If you have selected the date as 2016-03-15 in the till option, then the reports from the beginning till 15th March 2016 will be deleted.

4. Click **Delete**.

   Note: It is recommended to take backup of the reports before deletion.

Chapter

10

Notification

Notifications from the Seqrite Terminator informs 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 Terminator to receive notifications for different system events. Terminator supports the following two types of notifications:

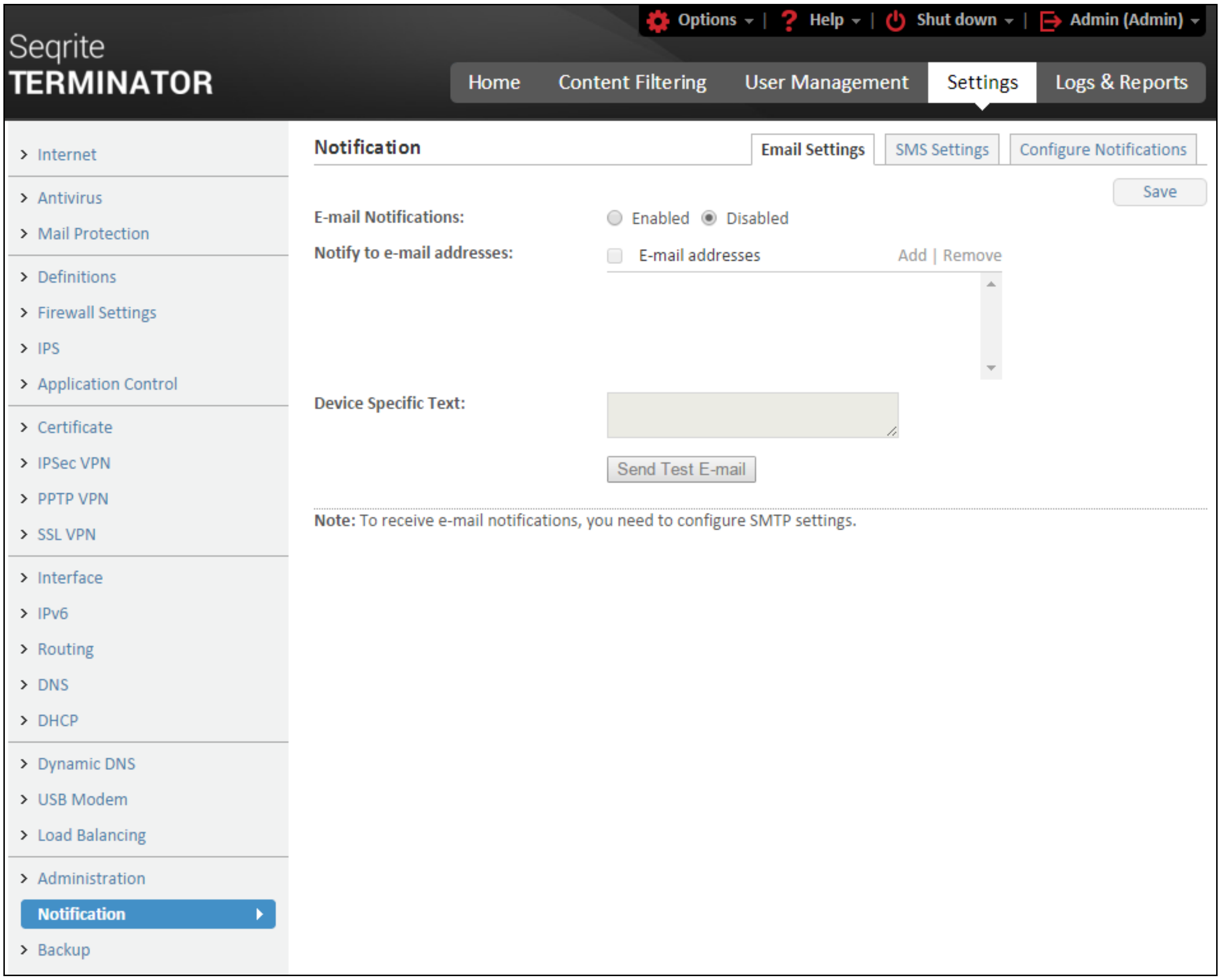
- Email Notification
- SMS Notification

Email notifications

You can configure Terminator 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. (See **SMTP Settings** for more details).

To configure email notifications follow the steps given below:

1. Log on to Seqrite Terminator **> Settings> Notifications**. The Email notifications configuration page is displayed.



Notification

E-mail Notifications: ○ Enabled ● Disabled

Notify to e-mail addresses: □ E-mail addresses Add | Remove

Device Specific Text:

Note: To receive e-mail notifications, you need to configure SMTP settings.

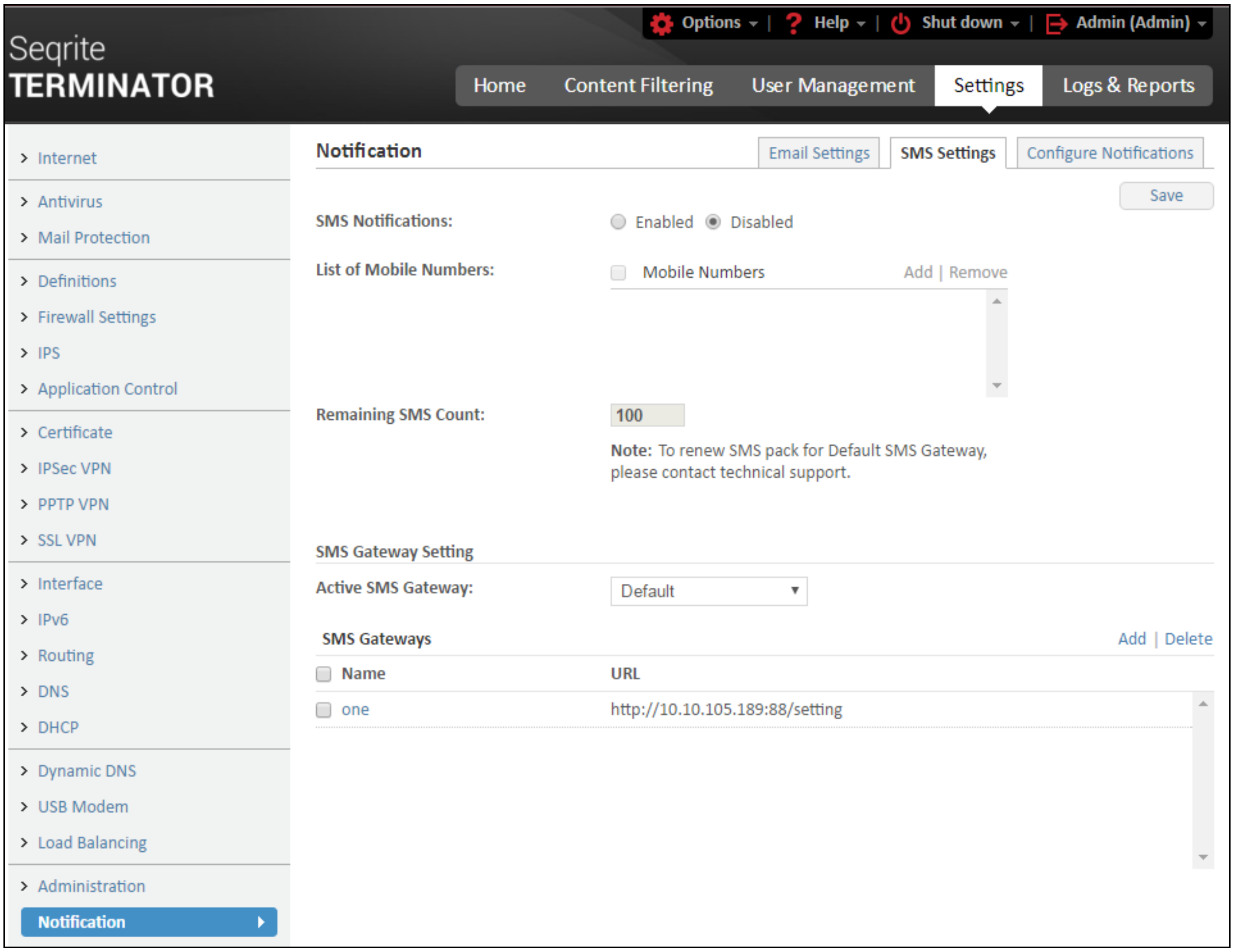
2. To enable email notifications, select **Enabled**.
3. Enter the **Notification from email address**. This is the email address from which you want to receive email notifications.
4. Enter the **Notify to e-mail addresses.** This is a list of e-mail addresses to whom email notifications will be sent. Use Add or Remove as required to maintain the list.
5. Enter the **Device specific text**. This can be a short description of the device from which notifications are sent.
6. Click **Send Test Mail**. A test mail is sent to the configured email addresses.

SMS notifications

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

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

1. Log on to Seqrite Terminator **> Settings > Notifications > SMS Settings**. The SMS notifications configuration page is displayed.



Notification

SMS Notifications: ○ Enabled ● Disabled

List of Mobile Numbers: □ Mobile Numbers Add | Remove

Remaining SMS Count: 100

Note: To renew SMS pack for Default SMS Gateway, please contact technical support.

SMS Gateway Setting

Active SMS Gateway: Default

SMS Gateways Add | Delete

□ Name	URL
□ one	http://10.10.105.189:88/setting

2. To enable SMS notifications, select **Enabled**.
3. Enter the mobile numbers that you want should receive the notification. Use **Add** or **Remove** as required to maintain the list.

   Note: For Default SMS gateway, the Country code supported are +91 & +971.
4. The **Remaining SMS** count displays the total number of SMS notifications that can be sent from the Terminator. These SMS count are displayed only for the Default SMS Gateway.
5. Select the **Active SMS Gateway**.

   You can select multiple SMS Gateway and click on Delete to delete the SMS Gateway(s).
6. Click **Save**.

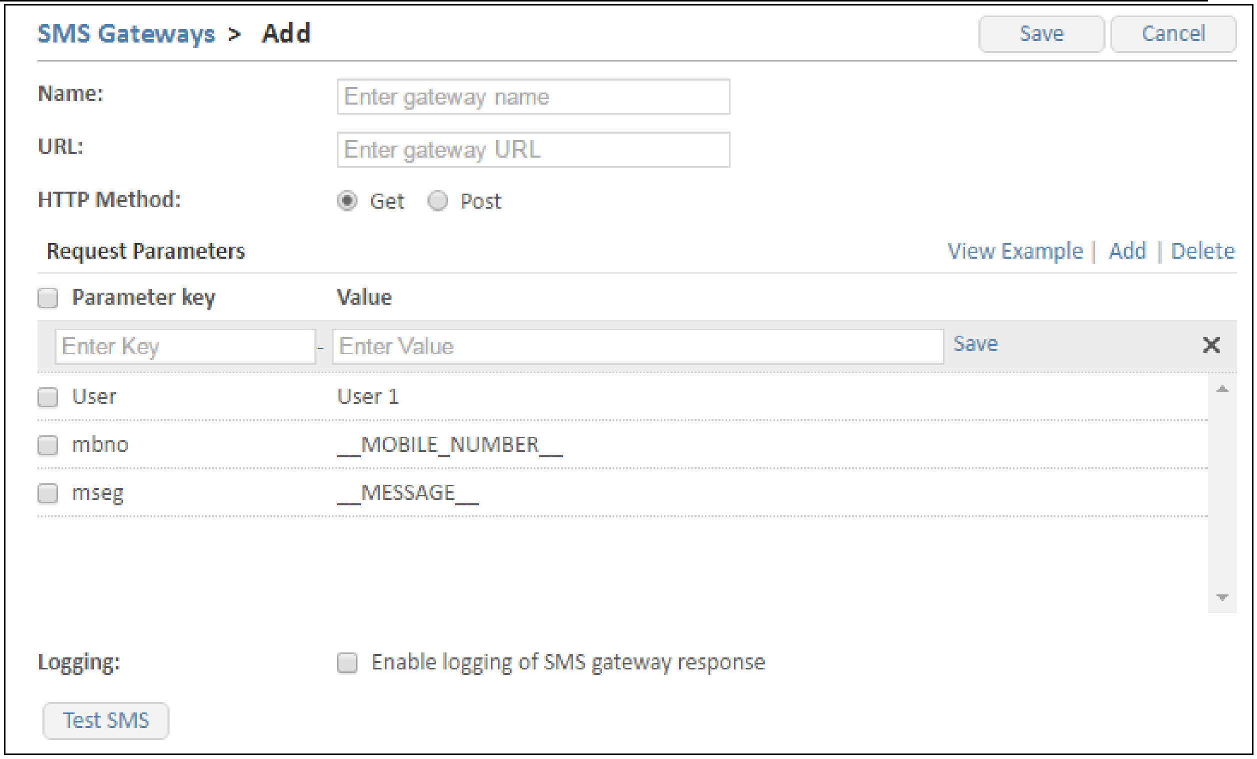
Add SMS Gateway

The Add SMS Gateway feature allows you to integrate third party SMS gateways in Terminator. By default, the Terminator is used to send notification SMS and guest user authentication.

To add an SMS gateway follow these steps:

1. Log on to Seqrite Terminator **> Settings > Notification> SMS Settings**.
2. In the SMS Gateway Settings section click **Add**.

   The SMS Gateway add page is displayed.



Name: Enter gateway name

URL: Enter gateway URL

HTTP Method: ● Get ○ Post

Request Parameters

□ Parameter key	Value
Enter Key	Enter Value
□ User	User 1
□ mbno	__MOBILE_NUMBER__
□ mseg	__MESSAGE__

Logging: □ Enable logging of SMS gateway response

3. Enter the **Name** for the gateway.
4. Enter the SMS gateway **URL**.
5. Select the **HTTP method**.
6. Add the Parameter key and its Value.

   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.

Place Holder	**Meaning**
__MESSAGE__	This place holder will be replaced by the message text while sending the SMS. The Message text may contain test SMS, notifications or guest user authentication.
__COUNTRY_CODE__	This place holder will be replaced by Country code while sending

	SMS.
__MOBILE_NUMBER__	This place holder will be replaced by mobile number while sending SMS.
__COUNTRY_CODE_MOBILE_NUMBER__	This place holder will be replaced by concatenated Country code and mobile number to represent receiver of the SMS.

However to configure third party SMS Gateway in Terminator, the following 2 placeholders are required and must be added under the Request Parameter:

__MOBILE_NUMBER__

__MESSAGE__

7. Select the **Logging** option if you want to enable logging of SMS gateway response.
8. Click **Test SMS** button, to send a test message to check if the SMS gateway is configured.
9. Click **Save** to save the SMS gateway configuration.

Edit SMS Gateway

To edit SMS gateway details follow these steps:

1. Log on to Seqrite Terminator **> Settings > Notification> SMS Settings**.
2. In the SMS Gateway Settings section click on the SMS gateway name.

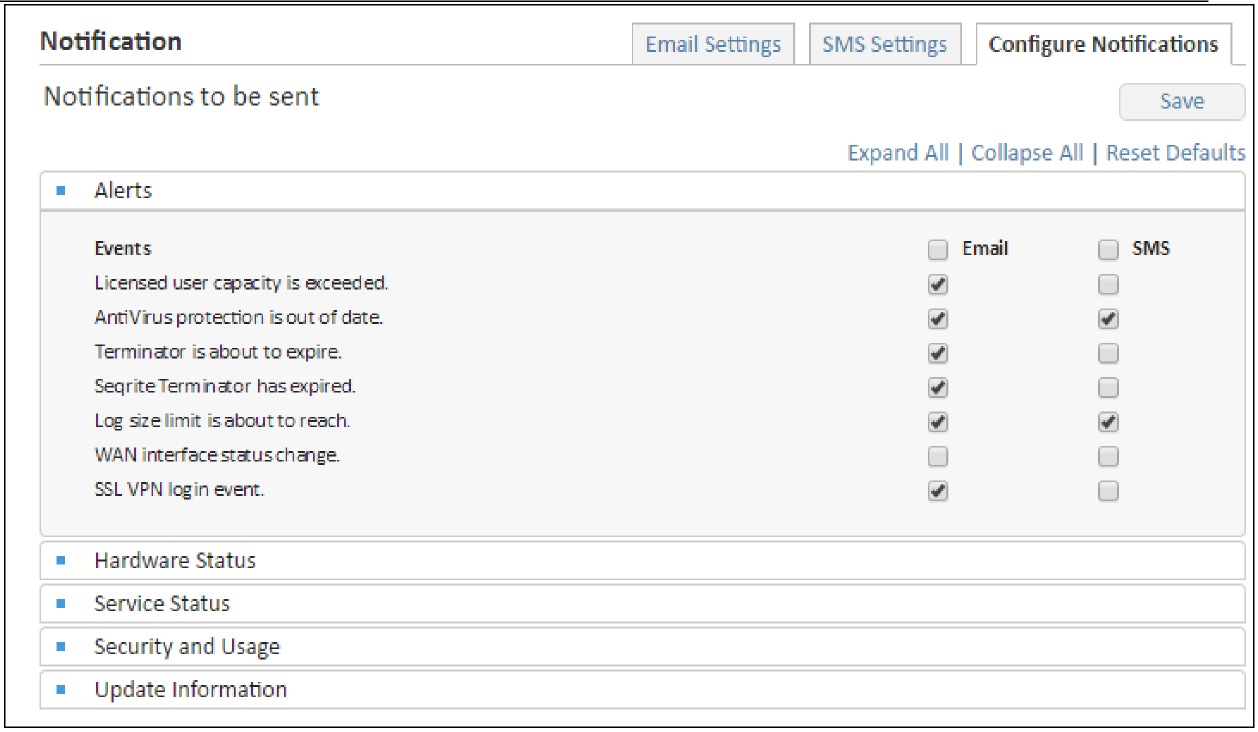
   The SMS Gateway edit page is displayed.
3. Make the required changes and click **Save**.

Notification Configuration

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.

To configure notification follow the steps given below:

1. Log on to Seqrite Terminator **> Settings > Notifications >Configure Notifications**. The notifications configuration page is displayed.



Events	□ Email	□ SMS
Licensed user capacity is exceeded.	☑	□
AntiVirus protection is out of date.	☑	☑
Terminator is about to expire.	☑	□
Seqrite Terminator has expired.	☑	□
Log size limit is about to reach.	☑	☑
WAN interface status change.	□	□
SSL VPN login event.	☑	□

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 Terminator 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 disk usage reaches 85%, notification is sent. Also, if CPU usage reaches 90%, a notification is sent.

   Service Status: If crucial services stops 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 Terminator 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.

Chapter

11

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 Terminator using the CLI

The Command Line Interface (CLI) console provides a collection of tools to administer, monitor and control certain Seqrite Terminator components. There are two ways to access Seqrite Terminator using the CLI console:

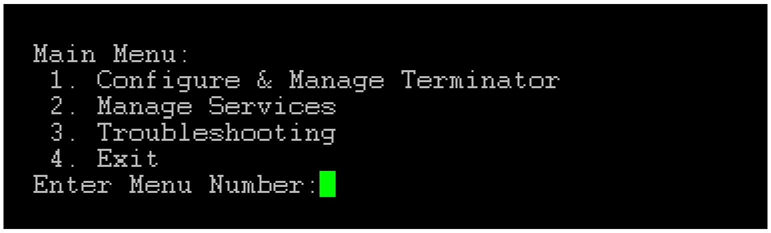
Direct Console connection: This can be done by attaching a keyboard and monitor directly to the Seqrite Terminator.

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.



```
Main Menu:
 1. Configure & Manage Terminator
 2. Manage Services
 3. Troubleshooting
 4. Exit
Enter Menu Number:
```

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.

The following table explains various menus:

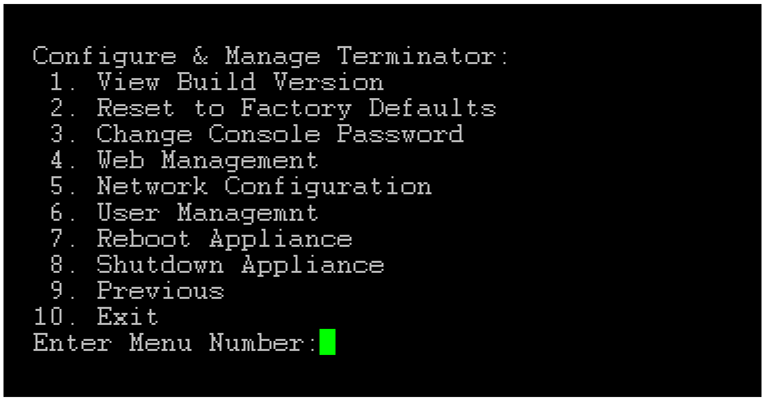
Menu	Description
Configure and manage terminator	Helps to configure and manage various services available on Terminator.
Manage Services	Helps to manage various services of Terminator.
Troubleshooting	Helps to troubleshoot various services.
Exit	To exit the CLI console.

Configure and manage Terminator

Seqrite Terminator CLI console provides option to configure and manage various services that are available.

To configure and manage terminator follow the steps given below:

1. Log in to Command Line Interface **> Configure and Manage Terminator.**



```
Configure & Manage Terminator:
 1. View Build Version
 2. Reset to Factory Defaults
 3. Change Console Password
 4. Web Management
 5. Network Configuration
 6. User Managemnt
 7. Reboot Appliance
 8. Shutdown Appliance
 9. Previous
10. Exit
Enter Menu Number:
```

The following table explains various menus:

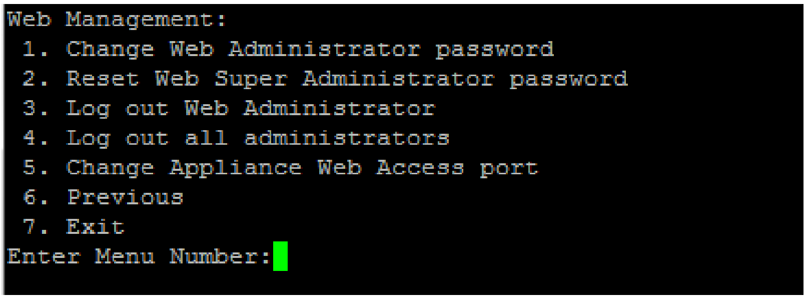
Menu	Description
View Build Version	Use this option to view the Seqrite Terminator build version.
Reset to Factory Defaults	Use this option to reset the Seqrite Terminator settings to factory defaults.
Change Console Password	Use this option to change the console password.
Web Management	Use this option to explore various options available under Web Management.

Network Configuration	Use this menu to configure your network.
User Management	Use this menu to manage Seqrite Terminator users.
Reboot Appliance	Use this option to reboot the Seqrite Terminator appliance.
Shutdown Appliance	Use this option to shut down the Seqrite Terminator appliance.

Web Management

CLI console provides various options for Web Management

1. Log in to Command Line Interface > **Configure and Manage Terminator > Web Management**.



```
Web Management:
 1. Change Web Administrator password
 2. Reset Web Super Administrator password
 3. Log out Web Administrator
 4. Log out all administrators
 5. Change Appliance Web Access port
 6. Previous
 7. Exit
Enter Menu Number:
```

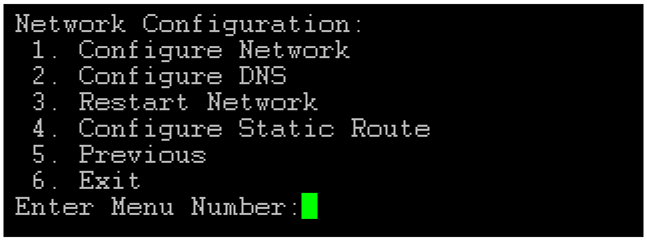
The following table explains the options available under Web Management:

Menu	**Description**
Change Web Administrator Password	Use this option to change the Terminator Web Administrator password.
Reset Web Super Administrator Password	Use this option to reset the Seqrite Terminator 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 Terminator 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 Terminator > Network Configuration.**



```
Network Configuration:
 1. Configure Network
 2. Configure DNS
 3. Restart Network
 4. Configure Static Route
 5. Previous
 6. Exit
Enter Menu Number:
```

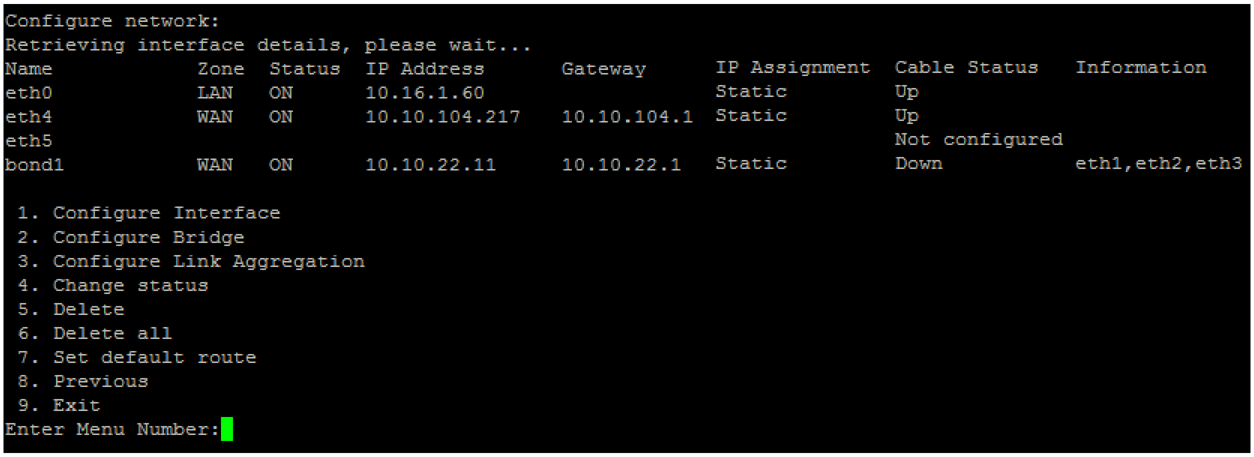
The following table explains the options available under Network Configuration:

Menu	Description
Configure Network	Use this option to configure the Seqrite Terminator 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

To configure Seqrite Terminator network through CLI console follow the steps given below:

1. Log in to Command Line Interface **> Configure and Manage Terminator > Network Configuration> Configure Network.**



```
Configure network:
Retrieving interface details, please wait...
Name            Zone  Status  IP Address       Gateway      IP Assignment  Cable Status   Information
eth0            LAN   ON      10.16.1.60                    Static         Up
eth4            WAN   ON      10.10.104.217    10.10.104.1  Static         Up
eth5                                                                       Not configured
bond1           WAN   ON      10.10.22.11      10.10.22.1   Static         Down           eth1,eth2,eth3

 1. Configure Interface
 2. Configure Bridge
 3. Configure Link Aggregation
 4. Change status
 5. Delete
 6. Delete all
 7. Set default route
 8. Previous
 9. Exit
Enter Menu Number:
```

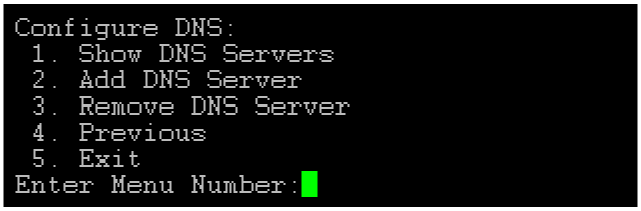
This option retrieves the interface details and provides various options as explained in table below

Menu	Description
Configure Interface	Use this option to configure the Seqrite Terminator interface.
Configure Bridge	Use this option to configure a bridge over two interfaces.
Configure Link Aggregation	Use this option top configure Link Aggregation interface.
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 Terminator > Network Configuration > Configure DNS.**



```
Configure DNS:
 1. Show DNS Servers
 2. Add DNS Server
 3. Remove DNS Server
 4. Previous
 5. Exit
Enter Menu Number:
```

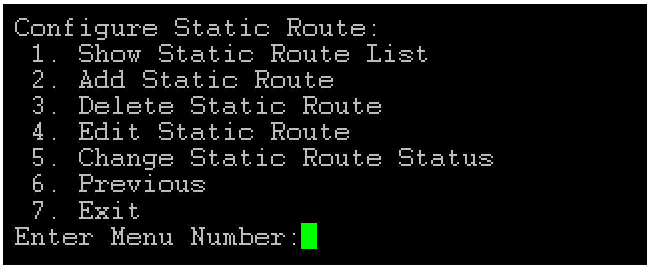
The following table explains various menus available under Configure DNS:

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 Terminator 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 Terminator > Network Configuration > Configure Static Route.**



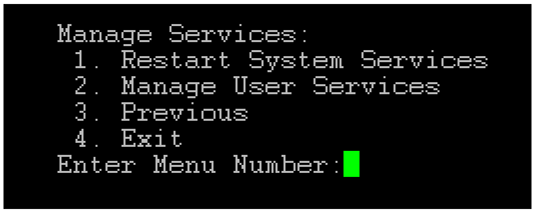
```
Configure Static Route:
  1. Show Static Route List
  2. Add Static Route
  3. Delete Static Route
  4. Edit Static Route
  5. Change Static Route Status
  6. Previous
  7. Exit
Enter Menu Number:
```

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 Terminator as shown in the screenshot below:



```
Manage Services:
  1. Restart System Services
  2. Manage User Services
  3. Previous
  4. Exit
Enter Menu Number:
```

The following table explains various menus available under Manage Services:

Menu	Description
Restart System Services	Use this option to restart system services.

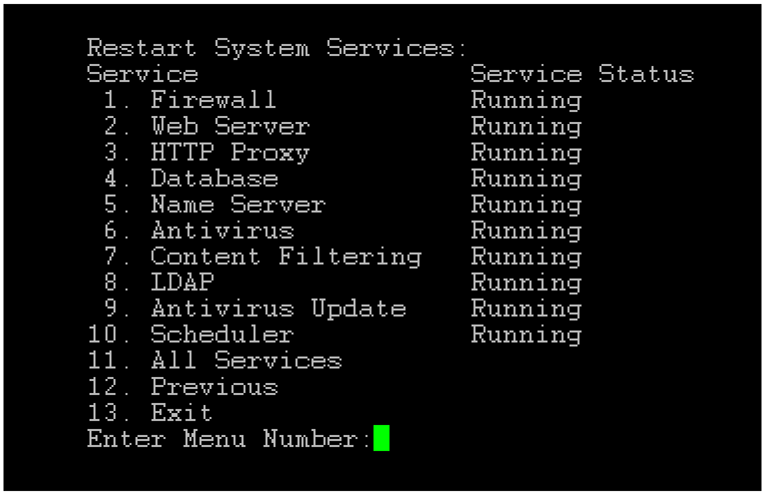
Menu	Description
Manage User Services	Use this option to manage user services such as: • IPS • Application control • Policy Based Routing

Restart System Services

Restart System Services allows you to restart any of the system services through CLI.

To restart services follow the steps given below:

1. Command Line Interface > **Manage Services > Restart System Services**.



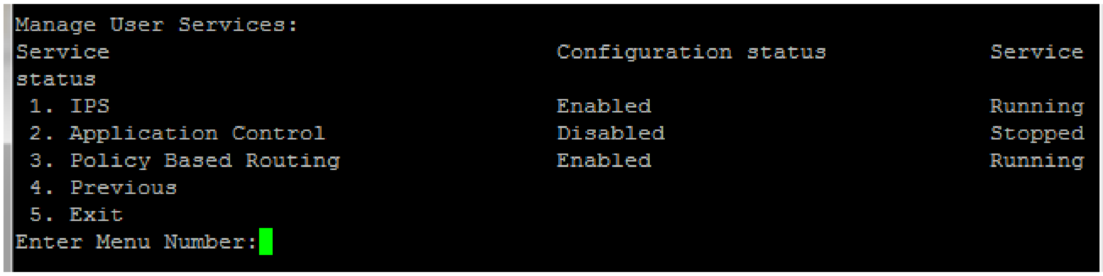
```
Restart System Services:
Service                 Service Status
 1. Firewall            Running
 2. Web Server          Running
 3. HTTP Proxy          Running
 4. Database            Running
 5. Name Server         Running
 6. Antivirus           Running
 7. Content Filtering   Running
 8. LDAP                Running
 9. Antivirus Update    Running
10. Scheduler           Running
11. All Services
12. Previous
13. Exit
Enter Menu Number:
```

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.**



```
Manage User Services:
Service                                 Configuration status            Service
status
 1. IPS                                 Enabled                         Running
 2. Application Control                 Disabled                        Stopped
 3. Policy Based Routing                Enabled                         Running
 4. Previous
 5. Exit
Enter Menu Number:
```

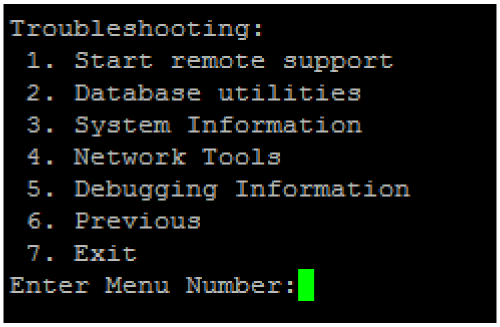
The following table explains various menus available under Manage User Services:

Menu	Description
IPS	Use this option to enable, disable or restart IPS.

Menu	Description
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 Terminator provides options to troubleshoot various services of as shown in following figure.

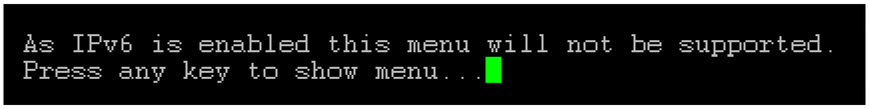


```
Troubleshooting:
 1. Start remote support
 2. Database utilities
 3. System Information
 4. Network Tools
 5. Debugging Information
 6. Previous
 7. Exit
Enter Menu Number:
```

The following table explains the commands used for troubleshooting:

Menu	Description
Start Remote Support	Use this option to start the remote support.
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 Terminator.
Network Tools	Use this option to view the available network tools.
Note: If IPv6 is enabled, following modules from CLI console will not be accessible: Configure & Manage Terminator >> Reset to Factory Defaults Configure & Manage Terminator >> Network Configuration Troubleshooting	

The following message is displayed if IPV6 is enabled on system.

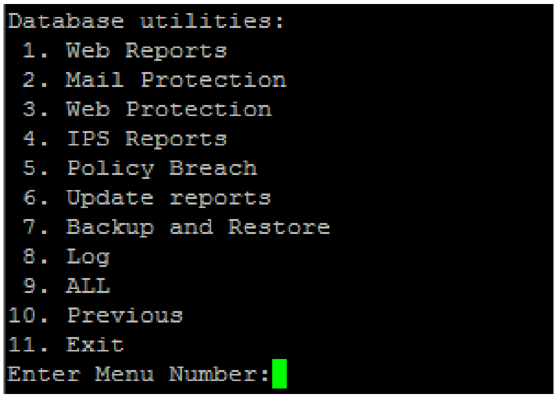


```
As IPv6 is enabled this menu will not be supported.
Press any key to show menu...
```

Troubleshooting Database Utilities

To troubleshoot Database Utilities follow the steps given below:

1. Log in to Command Line Interface **> Troubleshooting > Database Utilities**.
2. Terminator CLI console provides various database utilities as shown in figure below



```
Database utilities:
 1. Web Reports
 2. Mail Protection
 3. Web Protection
 4. IPS Reports
 5. Policy Breach
 6. Update reports
 7. Backup and Restore
 8. Log
 9. ALL
10. Previous
11. Exit
Enter Menu Number:
```

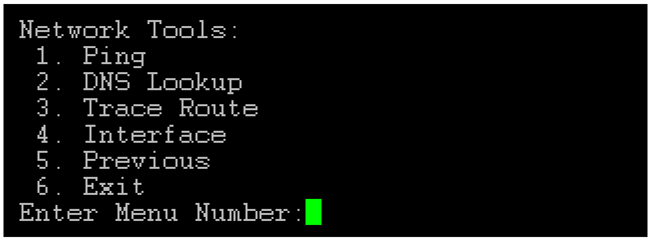
The following table explains various menus available under Database Utilities:

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.
Backup and Restore	Use this option to repair or clean database for Backup and Restore.
Log	Use this option to repair or clean database for log.
All	Use this option to repair or clean database for all the modules.

Troubleshooting Network Tools

To troubleshoot Network tools follow the steps given below:

1. Log on to Command Line Interface **> Troubleshooting > Network Tools.**



```
Network Tools:
  1. Ping
  2. DNS Lookup
  3. Trace Route
  4. Interface
  5. Previous
  6. Exit
Enter Menu Number:
```

The following table explains the various menus available under Network Tools

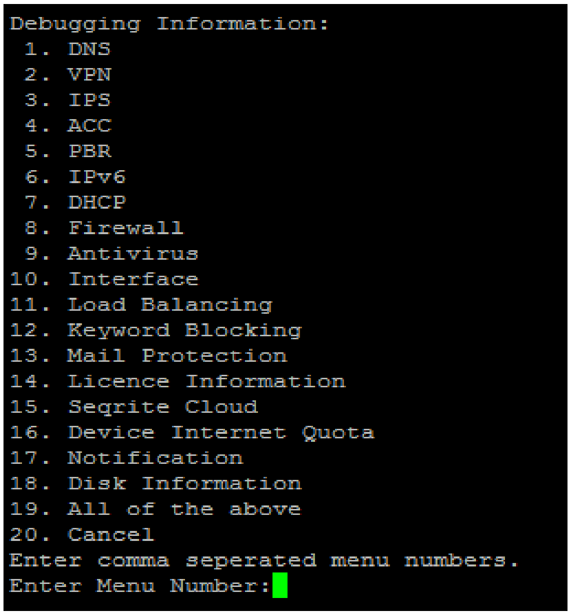
Menu	**Description**
Ping	Use this option to ping a particular IP address.
DNS Lookup	Use this option to lookup a particular IP address.
Traceroute	Use this option to route packets trace to network host.
Interface	Use this option to get all the necessary information about configured interfaces.

Troubleshooting Debugging Information

Seqrite Terminator allows you to collect debugging information that is the configuration files, log files, service status and database records of different modules, which can be used for troubleshooting. This debugging information should be downloaded and sent to the support team.

To get the debugging information follow these step:

1. Log in to Command Line Interface **> Troubleshooting > Debugging Information.** List of modules is displayed.



```
Debugging Information:
 1. DNS
 2. VPN
 3. IPS
 4. ACC
 5. PBR
 6. IPv6
 7. DHCP
 8. Firewall
 9. Antivirus
10. Interface
11. Load Balancing
12. Keyword Blocking
13. Mail Protection
14. Licence Information
15. Seqrite Cloud
16. Device Internet Quota
17. Notification
18. Disk Information
19. All of the above
20. Cancel
Enter comma seperated menu numbers.
Enter Menu Number:
```

2. Type the number corresponding to the module against **Enter Menu Number** and press **Enter**. Incase you want debugging information of multiple modules, enter comma separated menu numbers.
3. The debugging information will be collected in a .dbg file and a URL will be generated.
4. Enter the URL in browser to download the debugging information file. Once the download is completed share it with the support team.

Chapter

12

Support

Using the Support page you can report a problem or issue related to the Terminator. The following support are available:

Troubleshooting: Using the Diagnostic tools you can troubleshoot and check if the host/ IP address are available.

Email Support: Using this support type you can submit a ticket regarding the issue to the technical support team.

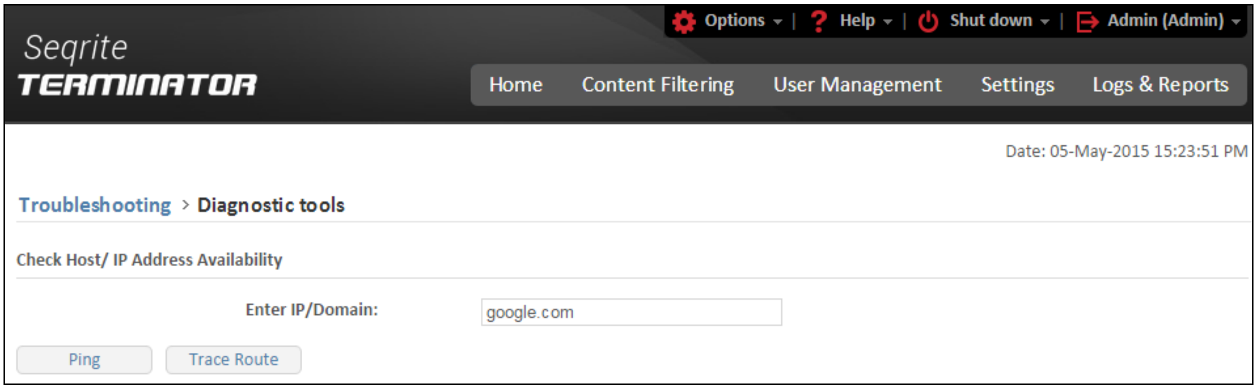
Phone support: Using this support type you can call the technical support center for instant support.

Remote Support: Using this support type you can allow the Support executive to connect and access your terminator device and troubleshoot the problem.

Troubleshooting

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. Logon to Seqrite Terminator **> Help > Support.** The Support page is displayed.
2. Click **Diagnostic tools**. The following page is displayed.



Date: 05-May-2015 15:23:51 PM

Troubleshooting > Diagnostic tools

Check Host/ IP Address Availability

Enter IP/Domain: google.com

3. Enter the **IP/Domain**.
4. Click **Ping** to check the reachability of host.
5. Click **Trace Route** to check the route (path) and transit delays of packets.

Email Support

This link can be used to submit a ticket regarding the issue faced in Seqrite Terminator. To submit a ticket follow these steps:

1. Log in to Seqrite Terminator**>** **Help** > **Support**.
2. Click **Submit Ticket**.

Phone Support

This feature helps you to call for instant support from the Seqrite technical experts.

Following is the contact number for phone support:

+91 92722 00121.

Timings for calling the support team is

Monday - Saturday

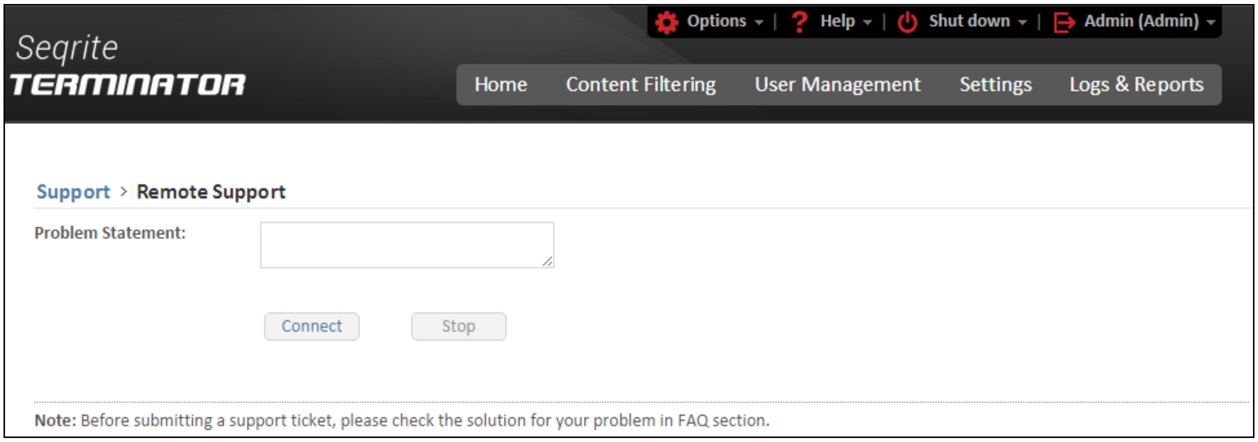
9:30 am to 9.30 pm (IST)

Remote Support

Seqrite Technical Support Team also provides Remote Support in some cases. This support module helps us to easily connect to your computer system through the Internet and provide technical support remotely. This helps Seqrite give you efficient support as our technical executives solves the issue for you.

To use Remote Support, follow these steps:

1. Log in to Seqrite Terminator**>** **Help** > **Support**.
2. Click the **Remote Support** button.



Note: Before submitting a support ticket, please check the solution for your problem in FAQ section.

3. Enter the **Problem Statement** and click **Submit Ticket**. The Seqrite Support executive will remotely access your system to fix the issue.

Support contacts

Seqrite provides extensive technical support for the registered users. It is recommended that you have all the necessary details with you during the call to receive efficient support from the Seqrite support executives.

When is the best time to call?

Seqrite provides technical support between 9:30 AM and 9:30 PM IST (India Standard Time).

Which number to call?

Seqrite users in India can call at +91 92722 00121.

Regional support for South India is available at +91 90431 21212 (Malayalam, Tamil, Telugu, and Kannada)

For support in other countries

To submit online queries and avail of the online chat facility, visit
http://www.seqrite.com/contact_support (24/7)

To check for the phone numbers in specific countries, visit
http://www.seqrite.com/int_techsupp

To check for the dealers in your country, visit http://www.seqrite.com/locate-dealer.

Details that are necessary during the call:

- Product Key is included inside the box of your product. If the product is purchased online, the product key 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? What were you doing when the problem appeared?

What should I say to the technical support personnel?

You need to be as specific as possible and provide maximum details as the support executive will provide solution based on your inputs.

Head Office Contact

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

A

Accessing Terminator 3
Adding a DHCP server 37
Adding a Static Route..41
Adding Administrators 128
Adding Definitions 20
Adding Static Lease 39
Admin Profiles...130
Admin Settings...127
Administrator...126
Alias 29
Antivirus.. 17, 103, 104, 159, 166
Application Control 120, 157
Authentication Servers 95

B

Backup 136
Bandwidth Usage 156
Blacklist..116
Bridge...73

C

Category Based Web site blocking.................................114
CLI 167
Command Line Interface..167
Common options..14
Configuring Interfaces..26
Content Filtering..103
Custom MIME Filtering 118

D

Dashboard..16
Date and Time setting..126
Default MIME Filtering...117
Definitions..20
Deleting a routing policy..46
Deleting Definitions 23
Deleting DHCP..40
Deleting interfaces...29
Device Management..126
DHCP 37
DNS 32
Domain name server..32
Dynamic DNS 35

E

Email notifications... 163
Enabling 6 to 4 tunnel 24
Enabling IPV6... 24
Enabling PBR 43
Exclusion.. 78

F

Factory reset 141
Failover.. 47
Flush DNS Cache 34

G

Global DNS Server 32
Group Management 89
Groups... 82
Guest User Settings 88

H

Head Office Contact.. 180

I

Identity Management.. 82
Interface 26
Internet Settings.. 78
Internet Usage... 147
Intrusion Prevention 154
Intrusion Prevention System 121
IPv6.. 23

K

Keyword Blocking 118

L

Link Aggregation.. 75
Load Balance 47
Log Viewer... 160
Logging in 3
Logs 147

M

Mail protection 105
Mail Protection 103, 147, 152, 175
MIME Filtering 117

N

Navigating 14
Network Configuration 20
Notification 163
Notification Configuration 165

O

On-line Support Ticket 178

P

PBR............42
Phone Support 178
Policy Based Routing............42
Policy Breach Attempts............155
Protection 103

R

Remote Support............178
Reports 147
Restore............136
Routing 41
routing policies............43

S

SMS notifications............164
SMTP Settings............133
Static DNS............34
Support............177

T

Terminator Features............1
Time Category 94
Troubleshooting 173

U

Unified Threat Management............ii, 1
Updates 159
URL Filtering 114
USB Modem 30
User Management............83
Users 82
UTM............1

V

Virtual Local Area Network 71
VLAN............71

W

Web Portal Customization 132
Web Protection 153
Web site access report 149
Whitelist 115
Wireless Universal Serial Bus 30