

**Quick Heal®**

*Security Simplified*

# **Administrator Guide**

## **Quick Heal Endpoint Security 5.2.1**

**QHEPS Total**  
**QHEPS Business**

Quick Heal Technologies (P) Ltd.  
<http://www.quickheal.com>

# Copyright Information

Copyright © 2012 Quick Heal Technologies (P) Ltd.

## **All Rights Reserved.**

All rights are reserved by Quick Heal Technologies (P) Ltd.

No part of this software may be reproduced, duplicated or modified in any form or incorporated into any information retrieval system, electronic or any other or transmitted in any form without prior permission of Quick Heal Technologies (P) Ltd, 603 Mayfair Towers II, Wakdewadi, Shivajinagar, Pune-411 005, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies (P) Ltd. is liable to legal prosecution.

## **Trademarks**

Quick Heal and DNAScan are registered trademarks of Quick Heal Technologies (P) Ltd.

# End-User License Agreement

## QUICK HEAL Endpoint Security 5.2.1 End-User License Agreement

### IMPORTANT

PLEASE READ THIS END-USER LICENSE AGREEMENT CAREFULLY BEFORE USING THIS SOFTWARE.

BY USING THIS SOFTWARE OR BY CLICKING THE "I AGREE" BUTTON OR LOADING OR ATTEMPTING TO LOAD THE QUICK HEAL SOFTWARE, IN ANY WAY (WILL CONSTITUTE A SYMBOL OF YOUR SIGNATURE), YOU ACKNOWLEDGE AND ADMIT THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO ALL THE TERMS AND CONDITIONS OF THIS END-USER LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS BELOW, DO NOT USE THIS SOFTWARE IN ANY WAY AND PROMPTLY RETURN IT OR DELETE ALL THE COPIES OF THIS SOFTWARE IN YOUR POSSESSION.

This License is a legally enforceable contract between you as an individual (assuming you are above 18 years and/or eligible to enter into an agreement), or the Company or any legal entity/organization that will be using the software (hereinafter referred to as 'you' or 'your' for the sake of brevity) referred to as the licensee, and Quick Heal Technologies Private Limited, Pune (hereinafter referred to as "Quick Heal" for the sake of brevity) and you shall have the right to use the software subject to the terms and conditions mentioned in this agreement or as amended by Quick Heal from time to time.

In consideration of payment of the License Fee, which is a part of the price, evidenced by the Receipt, Quick Heal grants the Licensee, a non-exclusive and non-transferable right. Quick Heal reserves all rights not expressly granted, and retains title and ownership of the Software, including all subsequent copies in any media. This Software 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.

### 1. DO'S & DON'TS

#### You can:

- Use one copy of the software on a single computer. In case of multi-users, use the software only on the said number of systems as mentioned on the packaging.
- Make one copy of the software solely for the backup purpose.
- Install the software on a network, provided you have a licensed copy of the software for each computer that can access the software over that network.

#### You cannot:

- Sublicense, rent or lease any portion of the software.
- Debug, decompile, disassemble, modify, translate, and reverse engineer the software.
- Try making an attempt to reveal/discover the source code of the software.
- Use for unlicensed and illegal purpose.

## **2. MANDATORY ACTIVATION**

Quick Heal warns you that in the process of installation of the software, the other security products/software installed on your computer may uninstall or be disabled if the same are not compatible with the Quick Heal software. The license rights granted under this Agreement are limited for the first twenty (20) days after you first install the Product unless you supply registration information required to activate your licensed copy as described in Activation Wizard of the Product. You can activate the Product through the Internet or telephone; toll charges may apply. You may also need to reactivate the Product if you happen to re-install the product due to some reasons. There are technological measures in this Product that is designed to prevent unlicensed or illegal use of the Product. You agree that we may use those measures. You agree that the Quick Heal software may use the measures that can control and prevent piracy of software. As a registered user, you are entitled to receive free (i.e. free of cost) virus database updates and free (i.e. free of cost) version upgrade (whenever Quick Heal releases new version upgrade) during the License period, subject to the terms and conditions mentioned herein.

As the only warranty under this Agreement, and in the absence of accident, abuse or misapplication, Quick Heal warrants, to the original Licensee only, that the disk(s) on which the software is recorded is free from defects in the materials and workmanship under normal use and service for a period of thirty (30) days from the date of payment as evidenced by a copy of the Receipt. Quick Heal's only obligation under this Agreement is, at Quick Heal's option, to either (a) return payment as evidenced by a copy of the Receipt or (b) replace the disk that does not meet Quick Heal's limited warranty and which is returned to Quick Heal with the copy of the Receipt.

## **3. THIRD PARTY WEBSITE LINKS**

At some point the software product may include links to third party sites; you may link to such third party websites as the user of this software. The third party sites are not under the control of Quick Heal and Quick Heal is not responsible for the contents of any third party website, any links contained in the third party websites. Quick Heal is providing these links to the third party websites to you only as a convenience and is not responsible for any kind of loss/ damage arising out of it.

## **4. SUPPORT**

Quick Heal offers support features during usage of this software with technical support team and/ or the technical support team may, at your discretion, take remote computer access. The availing of this support will be solely at your discretion and you are solely responsible to take the back-up of the existing data/software/programs on your computer before availing such a support and you are liable to bear all the direct, indirect and consequential cost associated to it. Quick Heal 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 it is beyond their scope, it will be the sole discretion of Quick Heal to suspend, cease, terminate or refuse such support as Quick Heal does not claim any warranty and/or guarantee of any kind in providing the support feature.

## **5. EMAIL/ELECTRONIC COMMUNICATION**

Once you register the software by activating the software product, Quick Heal may communicate with you on the contact information submitted during the registration process through email or other electronic communication device like telephone or a cell phone. The communication can be for the purpose of product renewal or product verification for your convenience.

## 6. QUICK HEAL STATUS UPDATE

Upon every update of licensed copy, Quick Heal Update module will send current product status information to Quick Heal Internet Center. The information that will be sent to the Internet Center includes the Quick Heal protection health status like, which monitoring service is in what state in the system. The information collected does not contain any files or personal data. 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 till the expiry date of the license.

## 7. COLLECTION OF INFORMATION

Quick Heal's software may collect the following information which may / may not contain any personally identifiable information either with or without your discretion/permission, solely for statistical purpose or enhancing and evaluating the ability, effectiveness and performance of Quick Heal's product in identifying and/or detecting the malicious behavioral pattern, inherently fraudulent websites and other Internet security threats/ risks. This information will not be correlated with any personally identifiable information and shall include, but not limited to:

- Any type of executable files which the Quick Heal software may identify having a potentially malware behavioral pattern.
- Any type of information relating to the status of the software that whether there occurred any error while installing the software or the installation was successful.
- Any type of URLs of websites visited that the Quick Heal software deems inherently and potentially fraudulent.
- Any type of information that the Quick Heal software deems potentially fraudulent, posing security risks/ threats.
- Any type of information for identifying the Media Access Control (MAC) address of the Computer on which the Quick Heal Software has been installed.
- Any type of information for identifying the Internet Protocol (IP) Address and information required for effective license administration and enhancing product functionality and usability.
- You admit that the information/data as collected above can be used for analyzing, preventing and detecting the potential internet security risks, publishing any type of data/ reports/ presentations on the trends collected, sharing the data to create awareness with any organizations, vendors.

## 8. INDEMNIFICATION

- a. You expressly understand, admit and warrant that in no event shall Quick Heal and/or any of its directors, employees, agents, partners, distributors be liable from any and against all claims, expenses, suits, costs, demands, judgments whatsoever made by you and/ or any third party for any direct, indirect, incidental, special, punitive, consequential and/or exemplary damages including, but not limited to damages for loss of business/profits, damages for loss of confidential/other information, failure to meet any statutory duty/duty of reasonable care/duty in good faith, economic/notional loss, loss for business interruption, goodwill, damage and loss of data or programs, or other intangible losses (even if Quick Heal has been advised of the possibility of such damages), to the fullest extent permissible by law:
  - i. Arising due to your usage of Software;
  - ii. Your negligence or inability of using the Software or support;
  - iii. Any dispute between you and third party with respect to availing the Software;

- iv. Your violation of any rights of any other individual and/or entity;
  - v. Your breach of the Agreement;
  - vi. Your violation of any provisions under any acts in India or abroad;
  - vii. The failure of Quick Heal to provide Support Service or any other service/information.
- b. This limitation will apply to all causes of action whether arise in equity or tort, including but not limited to breach of contract, breach of warranty, negligence, strict liability, misrepresentations and hereby release Quick Heal and/or its directors, employees, agents, distributors from any and all obligations, liabilities in excess of the limitation stated herein.
- c. In the event, Quick Heal and/or its directors, agents, employees, distributors are found liable, You Understand and accept that the liability of Quick Heal and/or its directors, agents, employees, distributors shall be limited only up to and not exceed in any case the License fees incurred by You in acquiring the software from Quick Heal or its distributors/agents. This Clause shall survive the termination of this Agreement.

## 9. LIMITED WARRANTY AND DISCLAIMERS

The software provided by Quick Heal is “AS IS” and “AS AVAILABLE”

- a. Quick Heal does not warrant, make any representations that the software will work uninterrupted, timely, secure or error-free or shall meet any or all your requirements whether disclosed to Quick Heal or any of its directors, agents, distributors and employees. The entire risks, faults as to performance of the software, the responsibility for selecting the software to achieve your intended results, the results obtained from the Software shall be assumed by You.
- b. The disclaimers and limitations set forth herein will apply regardless of whether you accept the software.
- c. You understand and accept that the Software will substantially perform according to the specifications, descriptions stated in the User Manual, (as updated from time to time), subject to the following and Quick Heal expressly disclaims any and all liabilities arising from the following circumstances:
  - i. Any actions initiated by You or by third parties which were beyond the reasonable control of Quick Heal;
  - ii. Any failures, malfunctions, defects resulting from abuse, improper installation, theft, misuse, accident, operation or maintenance, natural calamity, alteration, power failures, casualty, repairs made by any other party than Quick Heal, alterations, neglect, non-permitted modifications, acts of terrorism, vandalism;
  - iii. The deficiencies, defects in Your computer and related infringements;
  - iv. Your violations of the terms and conditions described in the User manual or in this Agreement.

## 10. INTELLECTUAL PROPERTY

The software, source code, activation code, license keys, documentation, systems, ideas, information, content, design and other matters related to the software, trademarks are the sole proprietary and Intellectual Property rights of Quick Heal protected under the Intellectual property Laws and belongs to Quick Heal. Nothing contained in this Agreement grant to You any rights, title, interest to intellectual property, including without limitation any error corrections, enhancements, updates or modifications to the Software whether made by Quick Heal or any third party. You understand and acknowledge that you are provided with a License to use the software subject to the terms and conditions of this Agreement.

## 11. GENERAL

- a. **Force Majeure.** Quick Heal will not be liable for any delay or failure to fulfill its obligations hereunder that results from any natural calamity (such as earthquake, flood etc.), war, civil disturbance, government policies, or other cause/s beyond its control. Provided that Quick Heal shall endeavour to complete the task within a reasonable period after happening of any event as covered under such force majeure.
- b. **Legal Jurisdiction.** This agreement and any matter relating thereto shall be subject only to jurisdiction of Courts at Pune, India and shall be interpreted as per the terms of the law/s for the time being in force in India. Any dispute which may arise out of this Agreement, breach of terms and conditions under this Agreement, shall be settled by direct negotiations between You and Quick Heal. In the case of failure to resolve the dispute in the manner set out above within 30 days from the date when the dispute arose, the dispute shall be referred to a panel of three arbitrators, with Quick Heal appointing one arbitrator, You appointing one arbitrator and the arbitrators so appointed jointly nominating a third presiding arbitrator. The venue of arbitration shall be Pune. The arbitration proceedings shall be governed by the Arbitration and Conciliation Act, 1996 and Indian Laws and shall be conducted in the English language. The arbitrators shall also decide on the costs of the arbitration proceedings. To the extent possible, after the commencement of any arbitral proceedings the Parties shall continue to perform their respective obligations under this Agreement. The provisions of this Clause shall survive termination of this Agreement. Subject to the provisions of this Clause, the Courts in Pune, India shall have exclusive jurisdiction and the parties may pursue any remedy available to them at law or equity.
- c. **Complete Agreement.** This Agreement comprises the entire agreement between the parties regarding the subject matter, and supersedes any proposals, communications or advertising, oral or written, with respect to the Software or subject matter of this Agreement. You shall be bound by any and all clauses of the Agreement updated and displayed by Quick Heal on [www.quickheal.com](http://www.quickheal.com) (the website) from time to time and the Agreement displayed on the website (from time to time) will be the finally concluded and binding Agreement between You and Quick Heal for all legal purposes which includes your each activation, re-activation and renewal of this Software. In case of any dispute/queries arising out of any translated versions of this Agreement, Quick Heal hereby expressly specifies and confirms that the English version as displayed on the website will be final for interpretation and the terms used, meaning conveyed in the English version will be authoritative and binding. Any waiver by either party of any violation of any provision of this agreement by the other party will not be deemed to waive any other violation of the same or any other provision.
- d. **Severability.** If any of the provisions contained in this Agreement is found by a court of competent jurisdiction to be invalid, illegal or unenforceable in any respect, the validity, legality or enforceability of the remaining provisions contained herein shall not be in any way affected or impaired thereby and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent.
- e. **Survival.** The Clauses in this Agreement including but not limited to rights to License fees receivable, “Indemnification”, “Limited Warranties & Disclaimers” and “Intellectual Property” shall survive expiration or termination of this Agreement.
- f. You cannot assign your rights or delegate duties or obligations under this Agreement. The failure to exercise or delay in exercising a right or remedy by Quick Heal under this Agreement shall not constitute a waiver of the right or remedy or a waiver of any prior, concurrent or subsequent right or remedy.

- g. The Section numbers and headings are included merely for the convenience of the parties and are not to be construed in interpreting this Agreement.
- h. Quick Heal reserves the right to co-operate with any legal process and may provide documents, information related to your usage of the Software and your general usage of the Computer.




---

# About This Document

This Administrator Guide covers all the information about how to install and how to use Quick Heal Endpoint Security in the easiest possible ways. We have ensured that all the details provided in this guide are updated with the latest enhancements of the product.

The following list describes the conventions that we have followed to prepare this document.

Convention	Meaning
<b>Bold Font</b>	Anything highlighted in bold indicates that it is a menu title, window title, check box, drop-down box, dialog, button names, hyperlinks, and so on.
	This symbol indicates additional information or important information about the topic being discussed.
<Step 1> <Step 2>	The instruction mentioned in the numbered list indicates actions that you need to perform.

---

# Contents

<b>Chapter 1. Introducing Quick Heal Endpoint Security .....</b>	<b>1</b>
How Does Quick Heal Endpoint Security Work? .....	2
Network Deployment Scenarios .....	3
<i>Scenario 1</i> .....	3
Title .....	3
Network Setup Description .....	3
Quick Heal Recommendation .....	4
<i>Scenario 2</i> .....	4
Title .....	4
Network Setup Description .....	4
Quick Heal Recommendation .....	5
<i>Scenario 3</i> .....	5
Title .....	5
Network Setup Description .....	5
Quick Heal Recommendation .....	6
<b>Chapter 2. Getting Started .....</b>	<b>7</b>
Prerequisites .....	7
System Requirements .....	7
Installing Quick Heal Endpoint Security on Windows Operating System.....	11
Installing Multiple Quick Heal Endpoint Security Server .....	14
<b>Chapter 3. Post Installation Tasks.....</b>	<b>17</b>
Registration .....	17
<i>Registering Online</i> .....	17
<i>Internet Settings</i> .....	18
Reactivation .....	18
<i>Reactivating Quick Heal Endpoint Security</i> .....	18
Configuring Update Manager .....	19
<i>How to Open Update Manager</i> .....	19
Uninstalling Quick Heal Endpoint Security.....	23
<b>Chapter 4. About Quick Heal Endpoint Security .....</b>	<b>24</b>
Home Page .....	24
<b>Chapter 5. Clients .....</b>	<b>27</b>
Client Status.....	27
Client Action .....	27
<i>Scan</i> .....	28
Scan Settings.....	29
<i>Update</i> .....	30
<i>Tuneup</i> .....	30

---

Tuneup Settings.....	31
<i>Application Control Scan</i> .....	32
Scan Settings.....	33
<b>Chapter 6. Client Deployment.....</b>	<b>34</b>
Through Active Directory.....	34
<i>Synchronizing with Active Directory</i> .....	35
Exclusion.....	36
Remote Install.....	37
Notify Install.....	39
Client Packager.....	40
Login Script.....	41
<i>Installing Login Script</i> .....	41
<i>Opening Login Script Setup</i> .....	41
<i>Assigning Login Script</i> .....	41
Installing Quick Heal Endpoint Security on Mac Operating System.....	42
Installing Clients on Linux-based Systems.....	42
Disk Imaging.....	43
Firewall Exception Rules.....	44
Remote Uninstall.....	44
<b>Chapter 7. Manage Groups.....</b>	<b>46</b>
Adding a Group.....	46
Adding a Subgroup.....	46
Renaming a Group.....	47
Deleting a Group.....	47
Setting Policy to a Group.....	48
Changing Group of a Client.....	48
Importing from Active Directory.....	48
<b>Chapter 8. Manage Policies.....</b>	<b>50</b>
Understanding Security Policy Scenario.....	50
Creating Polices.....	52
<i>Importing and Exporting Policies</i> .....	53
<b>Chapter 9. Settings.....</b>	<b>54</b>
Client Settings.....	54
<i>Scan Settings</i> .....	54
Scanner Settings.....	55
Virus Protection Settings.....	56
DNAScan Settings.....	56
Block suspicious packed files.....	57
Automatic Rogueware Scan Settings.....	57
Disconnect Infected Clients from the network.....	57
Exclude Files and Folders.....	58
Exclude Extensions.....	59

---

<i>Email Settings</i> .....	59
Email Protection.....	60
Trusted Email Clients Protection.....	60
Spam Protection .....	60
<i>External Drives Settings</i> .....	63
External Drives Settings.....	63
Autorun Protection Settings .....	63
Mobile Scan Settings .....	64
<i>IDS/IPS</i> .....	64
<i>Firewall</i> .....	66
<i>Web Security</i> .....	68
Browsing Protection Settings .....	68
Phishing Protection Settings .....	69
Web Categories .....	70
<i>Application Control</i> .....	71
<i>Device Control</i> .....	73
<i>Update Settings</i> .....	75
<i>Internet Settings</i> .....	76
<i>General Settings</i> .....	77
Schedule Settings .....	78
<i>Client Scan</i> .....	78
<i>Application Control</i> .....	80
<i>Tuneup</i> .....	81
<b>Chapter 10. Admin Settings</b> .....	<b>83</b>
Server .....	83
<i>Password</i> .....	83
<i>Notification</i> .....	83
SMTP Settings.....	87
<i>Add Device</i> .....	87
<i>Redirection</i> .....	88
<i>Manage Users</i> .....	88
<i>General</i> .....	90
Inactive Clients.....	90
<i>Client Installation</i> .....	90
<i>Inactive Client Settings</i> .....	91
<b>Chapter 11. Reports</b> .....	<b>92</b>
Client.....	92
<i>Viewing Reports of Virus Scan</i> .....	92
Viewing Reports of AntiMalware Scan .....	93
Viewing Reports of Web Security .....	94
Viewing Reports of Tuneup.....	94
Viewing Reports of Device Control .....	95

---

Viewing Reports of Application Control.....	96
Viewing Reports of IDS/IPS.....	98
Viewing Reports of Firewall .....	99
<b>Server .....</b>	<b>100</b>
<b>Manage .....</b>	<b>100</b>
Managing Settings .....	101
Managing Export.....	101
Managing Delete Reports .....	102
<b>Chapter 12. Update Manager .....</b>	<b>103</b>
Update Manager Status .....	103
Update Manager Settings.....	104
Alternate Update Managers.....	104
<b>Chapter 13. License Manager .....</b>	<b>105</b>
Status.....	105
License Order Form .....	106
<i>Renew my license.....</i>	<i>107</i>
<i>Add license for new endpoints .....</i>	<i>107</i>
<i>Buy additional feature .....</i>	<i>108</i>
<b>Chapter 14. Technical Support.....</b>	<b>109</b>
Contact Quick Heal Technologies .....	110

# Introducing Quick Heal Endpoint Security

For every organization, security of valuable data and resources is of paramount concern. Today Web technology is an integral part of business processes for all organizations. This puts them more at risk from new and unknown threats and attacks. Quick Heal Endpoint Security (QHEPS) is designed to provide complete security solutions to small and enterprise-level networks against various kinds of malicious threats such as viruses, Trojans, worms, backdoors, spywares, riskwares, pornwares, and hackers.

QHEPS is a Web-based management solution that integrates desktops, laptops and network servers. It allows you to access all clients and servers in the network and manage them remotely. You can deploy antivirus software applications, configure security policies, signature pattern updates and software updates on the clients and servers. You can also monitor clients to check whether there are any policy breaches or security threats within the organization, and take appropriate actions for ensuring security across the networks.

Quick Heal Endpoint Security works on Client/Server architecture. For our convenience, we will refer to the system on which the Management Console is installed as 'Console' and all other workstations/nodes of the network as 'Clients'.

## **Client Status**

Displays the current status of the clients running on a server. Among other updates, the status of a computer system also includes the scanning policy applied to that computer, QHEPS installation date, when the protection software was last updated, and security features enabled.

## **Client Action**

Helps you scan computers, update virus database, tune up computer performance, and verify security compliance in your organization.

You can remotely scan individual computers or computers in a group, customize scan settings and stop scanning as per your preference. You can also improve the performance of your computer systems by cleaning up disk space, registry entries, and schedule defragmentation at next boot. You can update the QHEPS virus database for the computers and verify security compliance as whether any unauthorized applications are installed on any computers.

### **Client Deployment**

Helps you synchronize with Active Directory groups to deploy and install Endpoint Security Client on a computer remotely. It allows you to compress the Quick Heal client setup into a self-extracting file to simplify delivery through email, CD-ROM, or similar media. It also helps you enable the login script setup to deploy Client on remote systems when they log on to the selected domain. It also supports deployment through imaging and remote uninstallation of the clients.

### **Manage Groups**

Helps you manage computers in groups. You can create groups and subgroups to manage clients. Policies can be set, added, deleted, or renamed for a particular group. Clients can be moved from one group to another and groups can be imported from Active Directory.

### **Manage Policies**

Helps you create protection policies for scanning your systems and clients, receiving emails, blocking or allowing external drives and devices. You can also define rules for Firewall and web security, authorized and unauthorized applications and so on. Various protection policies can be created according to the requirements of different clients.

## **How Does Quick Heal Endpoint Security Work?**

Quick Heal Endpoint Security (QHEPS) works on the Client/Server architecture where the console manages all the client agents deployed on the network. The console and client agents can be installed on almost all flavors of Microsoft Windows operating systems. The client agents can also be installed on the machines with Linux and Mac operating systems (OS). For a detailed description of console and client agent system requirements and compatibilities, refer to [System Requirements](#) in Chapter 2, “Getting Started”, p - 7.

QHEPS helps the administrators deploy Quick Heal AntiVirus remotely on the specified computers, groups or domains, which are the part of the same domain. Whenever the server copy of Quick Heal AntiVirus is updated, all computers configured to update from the server will be automatically updated without user intervention. QHEPS monitors these processes so that an administrator can view the computers that have Quick Heal AntiVirus installed, the virus database date of Quick Heal, whether Virus Protection is enabled, and if viruses are active in the memory of workstations. If any virus is found active in the memory of a workstation, that workstation gets disconnected from the network. If it detects that Quick Heal is uninstalled from any workstation(s), it reinstalls Quick Heal remotely without user intervention. This keeps the computers and the network safe from virus threats.

## Network Deployment Scenarios

Network setup differs from organizations to organizations depending on their size and architecture. Some organizations prefer a simple network setup with one server and multiple clients while some others may prefer a network setup with subnets or DHCP servers. Also, an organization with a huge network setup may have a single server with multiple LAN cards catering to the needs of networks with different IP ranges.

Quick Heal realizes the challenges of varying network setups in different organizations. Therefore installation recommendation for three prominent network setups has been provided in the following section.

### Scenario 1

#### Title

Installing Quick Heal Endpoint Security on a network with subnets configured using static IP address

#### Network Setup Description

The entire network is configured using static IP addresses and the network comprises of subnets connected to the main server. Quick Heal Endpoint Security will be installed on the server and Quick Heal client agents will be deployed on the client systems in the subnet.

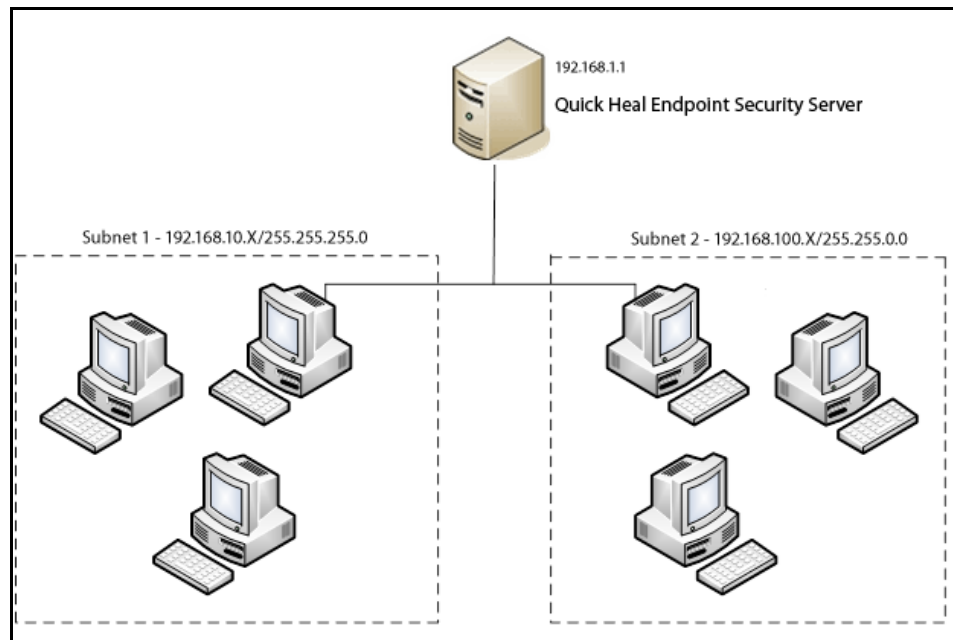


Figure 1: A network with subnets using static IP address



## Quick Heal Recommendation

- Before installation, ensure that the server and clients are connected. Verify this by pinging server to the clients and vice versa.
- The server system should be configured using static IP address.
- During installation of Quick Heal Endpoint Security, select **IP Address** in the **Server Information Screen**.

## Scenario 2

### Title

Installing Quick Heal Endpoint Security on a network with clients configured using DHCP server

### Network Setup Description

The entire network is configured using a DHCP server. Quick Heal Endpoint Security will be installed on server system and the Quick Heal client agents will be deployed on the client systems.

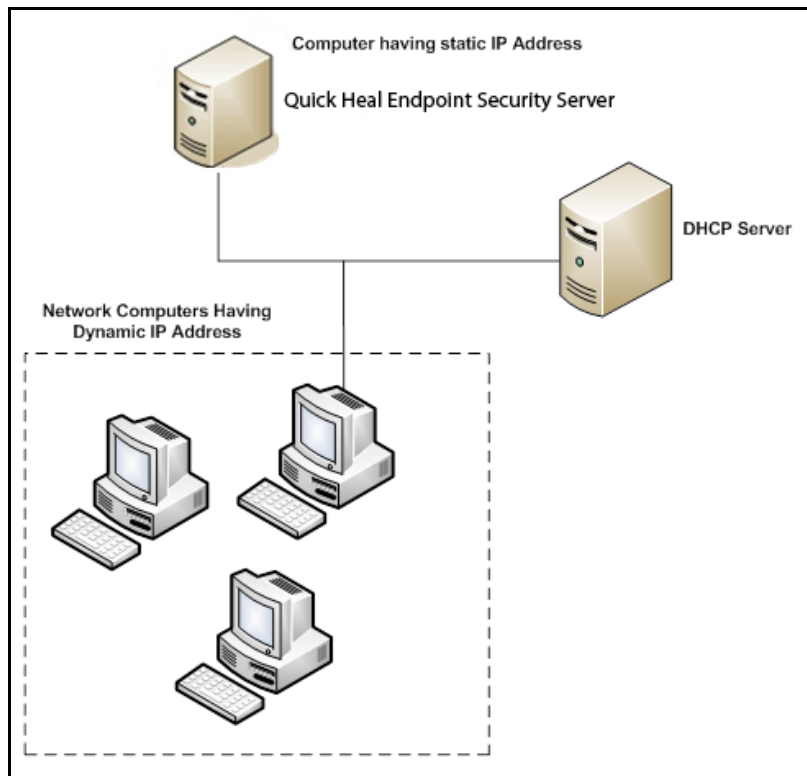


Figure 2: A network with clients using DHCP server

### Quick Heal Recommendation

- Before installation, ensure that the server and clients are connected. Verify this by pinging server to the clients and vice versa.
- The server system and the DHCP server system should be configured using static IP address.
- During installation of Quick Heal Endpoint Security, select **IP Address** in the **Server Information Screen**.

### Scenario 3

#### Title

Installing Quick Heal Endpoint Security on a server with two network cards

#### Network Setup Description

The server consists of two network cards, each catering to a network of different IP ranges (Ex: One network has the IP Range of 10.10.0.1 and the other network has the IP Range of 192.168.100.10). Quick Heal Endpoint Security will be installed on the server with two network cards and Quick Heal clients will be installed on all client systems of both the networks.

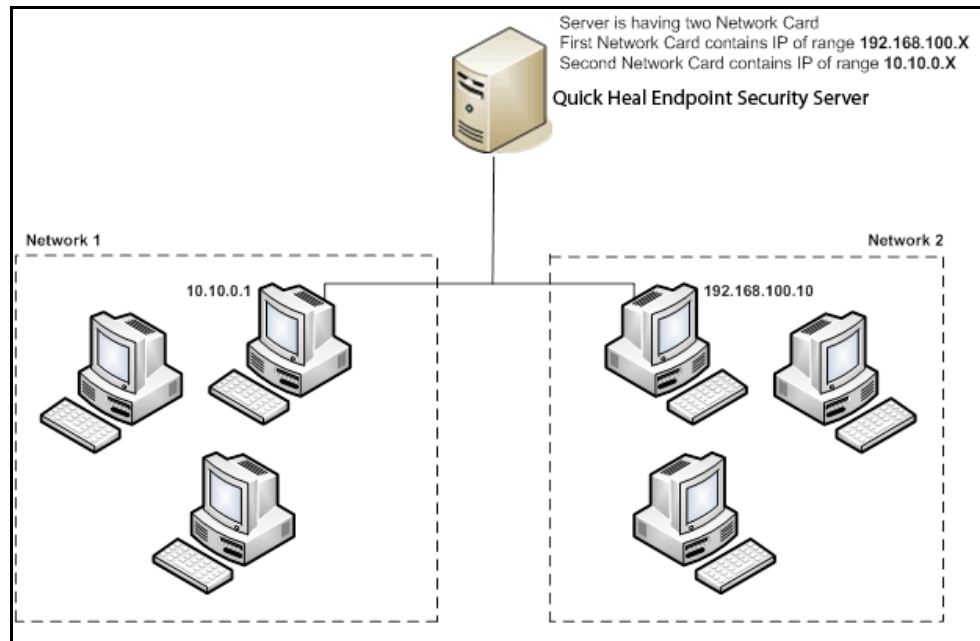


Figure 3: A server with two network cards

### Quick Heal Recommendation

- Before installation, ensure that the server and clients are connected. Verify this by pinging server to the clients and vice versa. Try to ping using IP address and system name.
- The server system should be configured using static IP address.
- During installation of Quick Heal Endpoint Security, select **Domain Name** in **Server Information Screen**. Provide the target server domain name. You can also use **Fully Qualified Domain Name (FQDN)** of the server if the client has access to a DNS server, which can resolve the FQDN with the client IP address.

## Chapter 2. **Getting Started**

Quick Heal Endpoint Security (QHEPS) is simple to install and easy to use. During installation, read each screen carefully and follow the instructions.

### **Prerequisites**

Remember the following guidelines before installing QHEPS on your computer:

- A machine with multiple antivirus software applications installed may result in system malfunction. We recommend you to remove any other antivirus software/hardware from your server and workstations before proceeding with the QHEPS installation.
- Close all open programs before proceeding with installing QHEPS.
- Network should be configured with TCP/IP protocols.
- To install on the server, you must have administrator or domain administrator rights on the server.
- In order to use Login Script Setup, Windows 2000 Server / Windows 2000 Advanced Server / Windows 2003 Server / Windows 2008 Server / Windows 2008 Server R2 / Windows Server 2012 should be properly configured with Active Directory services.

### **System Requirements**

Quick Heal Endpoint Security server can be installed on a system with any one of the following operating systems.

- Microsoft Windows 2000 SP 4 Professional / Server / Advanced Server
- Microsoft Windows XP Professional (32-bit/64-bit)
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)
- Microsoft Windows Vista Home Basic / Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter(64-bit)
- Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)

- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)

### **Minimum System Requirement for Console System**

- 1 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium processor or equivalent
- 1 GB of RAM
- 3225 MB of free disk space
- Monitor that supports 1024 x 768 resolution in 256-color mode.

### **Additional Software Required for Console System**

Console needs to have Web server services of either Microsoft IIS or Apache Web server on the system.

If Microsoft IIS is to be configured as Web server, the version requirements are as follows:

- IIS Version 5.0 on Windows 2000
- IIS Version 5.1 on Windows XP
- IIS Version 6.0 on Windows Server 2003
- IIS Version 7.0 on Windows Vista and Windows Server 2008
- IIS Version 7.5 on Windows 7 and Windows Server 2008 R2
- IIS Version 8.0 on Windows 8 and Windows Server 2012

If Apache is to be configured as Web server, the version requirement is as follows:

- Apache Web Server 2.0 or later

### **Other Essential Configuration on Console System**

- Administrator or Domain Administrator access on the console system.
- File and printer sharing for Microsoft Networks installed.
- Transmission Control Protocol/Internet Protocol (TCP/IP) support installed.
- Internet Explorer 7, 8, 9, or 10.

**Client side requirements****Windows Workstations supported**

- Microsoft Windows 2000 SP 4 Professional / Server / Advanced Server
- Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit/64-bit)
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)
- Microsoft Windows Vista Home Basic / Home Premium / Ultimate / Business / Enterprise (32-bit/64-bit)
- Microsoft Windows Server 2008 Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows Server 2008 R2 Web / Standard / Enterprise Datacenter (64-bit)
- Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)

**Mac Workstations supported**

- Mac OS X 10.6 or later
- Mac Computer with Intel Processor

**Linux Workstations supported****32-Bit:**

- Redhat 9
- Redhat Enterprise Linux 4,5,3,6.0
- Fedora 7,12,13, 14
- SuSE 7.3, SuSE ES 10, SuSE ES 11
- BOSS
- Mandrake 9.2
- Mandriva 2008
- CentOS 5
- Ubuntu 7.10, 10.04 LTS, 10.04.1 LTS

**64-Bit:**

- Redhat Enterprise Linux 5.3,6.0
- Fedora 13, 14
- SUSE ES 11
- Ubuntu 10.04 LTS, 10.04.1 LTS

**Minimum System Requirements for Windows Client**

- 256 MB of RAM
- 1800 MB of free disk space
- 1 GHz 32-bit (x86) or 64-bit (x64) processor for Windows Vista, Windows 2008 Server and Windows 7
- 1 GB of RAM for Windows Vista and Windows 7
- 512 MB of RAM for Windows 2008 and Windows 2008 R2
- For Windows 2000 – Service Pack 4 or later
- Internet Explorer 5.5 or later
- Administrative privilege is required for installation

**Minimum System Requirements for Mac Client**

- 512 MB of RAM
- 1200 MB free hard disk space

**Minimum System Requirements for Linux Client**

- 133 MHz or later Intel based (or compatible) processor
- 128 MB or later RAM
- 500 MB of free hard disk space

Note: The requirements outlined are minimum system requirements. We recommend that your system should have higher configuration to obtain best results.

To check for the latest system requirements, visit: [www.quickheal.com](http://www.quickheal.com).

## Installing Quick Heal Endpoint Security on Windows Operating System

To begin installation using the Quick Heal Endpoint Security DVD, follow these steps:

1. Insert the Quick Heal Endpoint Security DVD in the CD/DVD drive.
2. The autorun feature of the CD/DVD is enabled and it opens an installation screen automatically. Follow the instructions carefully.



Figure 4: Installation Screen

Sometimes the CD/DVD drive does not start automatically when DVD is inserted. In such a case, follow these steps for installation:

1. Double-click **My Computer** or the **Computer** icon on the Desktop.
2. Right-click CD/DVD drive and select **Explore**.
3. Double-click **Autorun.exe**.



---

To continue with installation, follow these steps:

1. On the installation screen, click **Install**.
2. On the installation wizard, click **Next**.

*The license agreement appears. Read the License Agreement carefully.*

3. Click **I agree** to accept the license agreement and then click **Next**.
4. Click **Browse** if you want to install Quick Heal Endpoint Security on a different location. To proceed with installation the default path, click **Next**.

*The Quick Heal Endpoint Security installer will scan your system for virus infection and verify the installed system components.*

5. Select one of the following Web servers:
  - i. **IIS Server:** Select IIS Server to install Quick Heal Endpoint Security on an existing IIS installation. If IIS Server is not installed /configured, you can proceed with the installation using Apache Web Server 2.0 provided in the Quick Heal Endpoint Security installer.
  - ii. **Apache Web Server:** Select Apache Web Server to install Apache 2.0 on an existing installation. If an Apache Web server version 2.0 or later installation is not found, Apache will be installed automatically.



Before installing the Apache Web server, refer to the Apache Web site for the latest information on upgrades, patches, and security issues: [www.apache.org](http://www.apache.org)

6. Click **Next**.
7. On the server information screen, select one of the following:
  - i. **Domain Name:** Provide the target server domain name. You can also use **Fully Qualified Domain Name (FQDN)** of the server if the client has access to a DNS server, which can resolve the FQDN with the client IP address.
  - ii. **IP address:** Provide the IP address of the target server. However, selecting IP address is not recommended if your network is configured using DHCP.
8. Under HTTP Port number, type a port to use as the server listening port. The Quick Heal Endpoint Security server address will be the following:  
`http://{Quick_Heal_Endpoint_Security_Server_name}:{port number}/qhscan502`
9. You can also enable Secured Socket Layer (SSL) security. Select the Enable Secure Socket Layer check box and type an SSL port number. If you enable SSL, this port number will serve as a listening port for the server. The Quick Heal Endpoint Security server address will be as follows:  
`https://{Quick_Heal_Endpoint_Security_Server_name}:{port number}/qhscan502`

10. Click **Next**.

*A message appears for your verification about the web server settings.*

11. To confirm, click **Yes**.

*You can make changes in your setting if required.*

*If you are "using a proxy server on your network" or "using Socks Version 4 & 5 network", you need to enter the IP address (or domain name) and port of the proxy, SOCKS V4 & SOCKS V5 server in the Connection settings. Username and password are mandatory to log on.*

*The following Quick Heal Endpoint Security modules require such changes: Registration Wizard, Update Manager, and Messenger. To enable and configure proxy settings:*

- i. Select **Enable proxy settings**.
- ii. Choose HTTP Proxy, Socks V 4 or SOCKS V 5 as per your settings and then do the following:
  - In Server, type IP address of the proxy server or domain name (For example: proxy.yourcompany.com).
  - In Port, type the port number of the proxy server (For example: 80).
  - In User name and Password, type your server logon credentials.

12. Click **Next**.

*The Client Settings screen appears.*

*Quick Heal will be installed on the client/workstation as per the path specified in this screen.*

13. Type the client Installation path. Path can be provided using either %PROGRAMFILES% or %BOOTDRIVE% variable. e.g. %PROGRAMFILES%\Quick Heal\Quick Heal or %BOOTDRIVE%\Quick Heal.

14. Specify the Client Agent Communication Port.

*The Quick Heal clients communicate with server to fetch important instructions such as scanning and updates, and submit the log to Endpoint Security Server using this Port Number, so ensure that this port number is not used by any other application in the network.*

15. Click **Next**.

*A message appears for your confirmation. You can change the port number if required.*

16. To confirm, click **Yes**.

*The Authentication screen appears.*

*Create Quick Heal Endpoint Security Administrator password to access the Web console and client password to access the client settings at the client side. Confirm the passwords in the text boxes. This helps prevent unauthorized users from accessing the Web console and make changes in your settings or remove the clients.*

*Passwords for Administrator and Clients must be created. However, the password for Administrator and Client should be different; else installation will not proceed.*

*The installation summary screen appears. You can change your settings if required.*

17. Click **Next**.

*A message appears stating that the Network connection on the system will be temporarily disabled if you continue with the Quick Heal Endpoint Security installation on the system.*

18. To continue with installation, click **OK**.

*The installation starts. Read the important information related to Quick Heal Endpoint Security.*

19. Click **Next**.

20. To register Quick Heal Endpoint Security and configure Update Manager, click **Next**. If you want to perform these tasks later, clear these options.

21. To complete the installation, click **Finish**.

## Installing Multiple Quick Heal Endpoint Security Server

Quick Heal Endpoint Security multiple server installation is a unique feature of Quick Heal Endpoint Security. Administrators can install latest version of Endpoint Security where the previous version is already installed. This feature enables Administrators to easily migrate to the latest version of Quick Heal Endpoint Security in simple ways.

### ***Upgrading previous version of Quick Heal Endpoint Security to the latest version***

Quick Heal Endpoint Security can be upgraded in the following way:

1. Install Quick Heal Endpoint Security on the system where previous version of Endpoint Security is installed.
2. Quick Heal Endpoint Security will detect the previous version and will show the following message:



Figure 5: Pre-install Scan

3. To proceed with multi-server installation, click **Yes**.

*After the installation of the latest version of Quick Heal Endpoint Security is complete, open the previous version of Quick Heal Endpoint Security and follow these steps:*

- i. Select **Admin Settings > Server > Redirection**.
- ii. In Server Name/IP text box, type the Server Name or IP Address of the latest version of Quick Heal Endpoint Security.
- iii. In Port text box, type the port number of the latest version of Endpoint Security.
- iv. Click **Apply**.

*This will send a notification about the latest version of Quick Heal Endpoint Security to all Quick Heal clients, which will be redirected to the latest version.*

4. The latest version of Quick Heal Endpoint Security will check if there are any previous version of clients in the network. If detected, Quick Heal Endpoint Security will automatically uninstall the previous version of clients and install the latest version.
5. Once all the clients are upgraded, you can uninstall the previous version of Quick Heal Endpoint Security from the system. Before uninstallation, note down the Product Key and Activation Number of your Quick Heal Endpoint Security that will be required for re-activation of the latest version of Quick Heal Endpoint Security.

6. After uninstallation of the previous version of Quick Heal Endpoint Security, re-activate the latest version of Quick Heal Endpoint Security with your existing Product Key and Activation Number.



- You can upgrade all the clients to the latest version within 30 days period only.
- If you have configured previous version of Quick Heal Endpoint Security site with IIS on Windows XP and 2K-based system and with SSL support enabled, you will not be able to configure later version of Quick Heal Endpoint Security site with SSL support on the operating systems mentioned in the preceding section. In this case, you can install the latest version of Quick Heal Endpoint Security with Apache Web Server.
- If you have installed a previous version of Quick Heal Endpoint Security, do not uninstall Apache Server during uninstallation of the previous version of Quick Heal Endpoint Security.

---

## Chapter 3. Post Installation Tasks

Quick Heal Endpoint Security must be registered immediately after installation to activate the copy; otherwise client deployment will not start.

### Registration

Quick Heal Endpoint Security is simple to register.

#### Registering Online

If your system is connected to the Internet, you can register Quick Heal Endpoint Security online in the following way:

1. Go to **Start > Programs > Quick Heal EPS Console 5.2.1 > Activate Quick Heal EPS Console**.
2. On the Registration Wizard, type the Product Key and then click **Next**.
3. Type relevant information in the **Purchased from, Register for** and **Name** text boxes and then click **Next**.
4. Type your personal details such as Company Email Address, Administrator Email Address, Contact Number, and location details.
5. Click **Next**.

*A confirmation screen appears with the information that you have entered. You can change your information if required. To change your information, click **Back** to go to the previous screen and make the required changes.*

6. To confirm, click **Next**.

*It takes a few seconds to register and activate your copy. Please stay connected to the Internet during this process.*

*After the activation completes successfully, a message appears with the License validity information for your reference.*

7. To close the Registration Wizard, click **Finish**.



You can find the Product Key on the User Guide or inside the box. If you have purchased the software online using credit card, you will find the Product Key in the email confirming your order.

## Internet Settings

When you open the registration wizard, the system tries to connect to the direct Internet connection. If the default Internet connection is not found, it shows the message “System is not connected to the Internet. Please connect to Internet and try again”.

If you have alternative ways to connect to the Internet, follow these steps to connect to the Internet and register online:

1. Click the **Internet Settings** button.

*The Configure Proxy Settings screen appears.*

2. To set the proxy setting for Internet, select **Enable Proxy Setting**.

*The proxy settings details are activated.*

3. In the Sever text box, type the sever name.

4. In the Port text box, type the port number.

*You can also set authentication rule if you use Firewall or proxy server. For this, type the User name and Password under Authentication.*

5. To save your setting, click **OK**.

6. Click **Retry** to connect to the Internet.

*If you get connected to the Internet, the online activation wizard opens and you can activate your product online.*

## Reactivation

### Reactivating Quick Heal Endpoint Security

Re-activation is a facility that ensures that you use the product for the full period till your license expires. Re-activation is very helpful in case you format your system when all software products are removed, or you want to install Quick Heal Endpoint Security on another computer. In such cases, you need to re-install and re-activate Quick Heal Endpoint Security on your system.

The re-activation process is similar to the activation process, with the exception that you need not type the complete personal details again. Upon submitting the Product Key, the details are displayed. You can just verify the details and complete the process.

Note: If your license has expired and you try to reactivate it, a message about it is displayed. You can renew your license by purchasing a renewal code.

## Configuring Update Manager

Update Manager is a tool integrated with Quick Heal Endpoint Security. It is used to download and manage the updates for Quick Heal Endpoint Security. It provides you the flexibility to download the updates on a single machine. All the Quick Heal Endpoint Security clients fetch the updates from this centralized location. It also provides the facility of automatically updating Quick Heal Endpoint Security for enhancements or bug fixes.

### How to Open Update Manager

To open Update Manager, select **Start > Programs > Quick Heal EPS Console 5.2.1 > Update Manager**.

Update Manager includes the following features:

#### **Status**

Status includes information about the latest updates downloaded by Update Manager. It displays the Version, Service Pack, and Virus Database Date of the Quick Heal product.

#### **Configuration**

Configuration helps you customize and configure Update Manager. To access Configuration, follow these steps:

1. Select **Start > Programs > Quick Heal EPS Console 5.2.1 > Update Manager**.
2. Click **Configuration**.
3. Type the Super Administrator and Password and then click **OK**.
4. If you want to take the updates automatically, select **Enable Automatic Updates**.

*This feature is enabled by default. It is recommended that you do not disable this feature.*



## 5. Select the update mode from the following:

- **Download from Internet Center** – Helps you download the updates to your system from the default Internet Center.
- **Download from specified URL:** Helps you take the updates from where the updates are downloaded in the system with Internet connection. If the system containing Update Manager is not connected to the Internet, it can use the updates downloaded by a connected system.
  - In Server, type the URL.
  - In Port, type the port number.

Note: msg32.htm file should be present at the update location where the updates are downloaded in the system with Internet connection.

To create msg32.htm file, rename a text file as msg32.htm file.

- **Pick from the specified path** – Helps you pick the updates from a specified folder of local system. This is helpful when your system is not connected to the Internet, you can specify the path of the local folder where the updates have been copied from other system.

For example, if you have downloaded the updates on other system, you can copy them into a CD/DVD or pen drive and then paste in the local folder and Update Manager will fetch the updates from this local folder path.

- Select the Pick from specified path option.
- Enter the path to the folder where the updates have been copied in the local system.
- **Download Endpoint Security Service Pack:** Helps you download the Quick Heal Endpoint Security Service Pack. By default, this feature is enabled.

## 6. Select one of the following:

- **Download updates to:** Helps you download the updates to the location as preferred by you. All Quick Heal Clients will take the updates from this centralized location.
- **Always take backup before downloading new update:** Helps you take the backup of the existing updates before new updates are downloaded. These backups are used in case a rollback to previous update is required. By default, this feature is enabled.
- **Delete report after:** Helps you delete the reports as per the time interval specified in the drop-down box. By default, this feature is enabled and the default value of time interval in the drop-down box is 10 days.

7. To prevent unauthorized access to settings, select Enable Password Protection and then configure it.
8. To save your changes, click **Apply**.
9. To restore the default settings, click the **Default** button.

Following are the two buttons that are accessible at all times:

- Update Now
- Rollback

Update Now	Helps you download the updates of Quick Heal Endpoint Security.
Rollback	Helps you take the Update Manager back to the previous update state. This feature will work only if <b>Always take backup before downloading new update option</b> is selected in the Configuration section of Update Manager. The steps for performing Rollback are as follows: <ol style="list-style-type: none"> <li>1. Click the <b>Rollback</b> button. The Quick Heal product for the Endpoint Security is displayed.</li> <li>2. Click Rollback.</li> </ol>

### ***Enabling password protection***

Enable Password Protection	This feature also allows you to change password of Update Manager. Enabling password protection prompts you to enter the password for the first time you access either Configuration or Connection Settings feature of Endpoint Security. To change the password, follow these steps: <ol style="list-style-type: none"> <li>1. Click the <b>Change Password</b> button.</li> <li>2. In Enter Old Password, type your existing Super Administrator Password.</li> <li>3. In Enter New Password, type your new password.</li> <li>4. In Confirm New Password, re-type your new password.</li> <li>5. To save your new password, click <b>OK</b>.</li> </ol>
----------------------------	--

### ***Connection Settings***

If a proxy server is being used on the network, you need to provide the IP address (or domain name) and the port number of the proxy server in the Connection Settings. To access Connection Settings, follow these steps:

1. Select **Start > Programs > Quick Heal EPS Console 5.2.1 > Update Manager**.
2. Click **Connection Settings**.
3. Type the Super Administrator **Password** and click **OK**.

To enable HTTP proxy settings, follow these steps:

1. In Connection Type list, select HTTP.
2. Select **Enable Proxy**.
3. In Proxy Type, select HTTP Proxy / Sock4 / Sock5.
4. In Server, type the IP address of the proxy server or domain name (e.g. proxy.yourcompany.com).
5. In Port, type the port number of the proxy server (e.g. 80).
6. If required, type your logon credentials in User Name and Password in Authenticate in case of firewall **or** proxy server section.
7. To save the changes, click **Apply**.
8. To restore the default settings, click the **Default** button.

### **Reports**

The Reports section includes a log of updates or rollback activity. It provides the details such as Date, Time, and Status of the updates or rollback activity. To access Reports, follow these steps:

1. Select **Start > Programs > Quick Heal EPS Console 5.2.1 > Update Manager**.
2. Click **Reports**.

You can perform the following actions on reports:

View	Select a report and click <b>View</b> to get the complete details of the downloaded update or rollback.
Delete	Select a report and click <b>Delete</b> to delete the report.
Delete All	Click <b>Delete All</b> to delete all the reports in the section.
Previous	Helps you view the previous report.
Next	Helps you view the next report.
Save As	Helps you save a copy of the report in text format on your local machine.
Print	Helps you take a printout of the report.
Close	Helps you exit from the report window.

## Uninstalling Quick Heal Endpoint Security

Uninstalling Quick Heal Endpoint Security may expose your systems and valuable data to virus threats. However, if you need to uninstall Quick Heal Endpoint Security, follow these steps:

1. Go to **Start > Programs > Quick Heal EPS Console 5.2.1 > Uninstall EPS Console**.

*Quick Heal Endpoint Security Uninstaller will prompt for the Password.*

2. Type Super Administrator Password.
3. Click **Next**.
4. Select **Restart System Now** to restart the system immediately or **Restart system later** to restart system later.
5. To complete uninstallation of Quick Heal Endpoint Security, click **Finish**.



- If you have assigned a script to install client by Login Script Setup to domain servers, clear it through the Login Script Setup before proceeding with uninstallation.
- If you have configured the Quick Heal Endpoint Security site with Apache Web Server, the uninstallation wizard will prompt you to uninstall Apache Web Server. Select Uninstall Apache Server only if no other site is running on Apache.
- Before proceeding with uninstallation, ensure that all other running programs are closed.

## Chapter 4. About Quick Heal Endpoint Security

Advanced graphical console gives current status of health of endpoints and highlights critical security situations that need immediate attention. This section explains how to navigate the web console.

To open the Web console:

- On any computer on the network, open a Web browser and type:  
http://{Quick\_Heal\_Endpoint\_Security\_Server\_name}:{port number}/qhscan502.
- If SSL is being used, type:  
https://{Quick\_Heal\_Endpoint\_Security\_Server\_name}:{port number}/qhscan502

The browser displays the Quick Heal Endpoint Security Home page.

- Type the user name as ‘administrator’ in the User Name text box and Super Administrator Password in the Password text box, and then click **Login**. The browser displays a summary of the Web console.

### Home Page

After logging on to the Quick Heal Endpoint Security console, the Home page appears from where you can access all the features and work. The Home page also displays a summary of the various activities described as follows:

**Quick Heal Endpoint Security:** Displays the software application version, Service Pack (if any).

**Endpoint Security Client:** Displays the client application version, Service Pack (if any), and Virus Database details.

**Threat Meter:** Displays current threat level of your network.

Following are the threat levels:

Normal	Indicates that 12% of the clients detected viral infection in last 24 hours.
Elevated	Indicates that 24% of the clients detected viral infection in last 24 hours.
High	Indicates that 36% of the clients detected viral infection in last 24 hours.
Critical	Indicates that more than 36% of the clients detected viral infection in last 24 hours.

Important: Thorough scanning of the entire network is recommended if the threat level is at High Alert or Critical.

**Alert:** An alert indicates an event that demands your action. Click **More** to see all the alerts. (The More link is displayed only if multiple alerts are available.) You can take appropriate action to fix the issue.

### Network Health

Graphical representation of the network health shows how secure the system is. This is displayed in four grids that have the following meanings:

Symbol	Level	Description
Green	Normal	Indicates system is not infected and is secure.
Yellow	Elevated	Indicates low level of system infection.
Orange	High	Indicates high level of system infection that requires immediate action.
Red	Critical	Indicates critical level of system infection that requires immediate action.

### View for:

Gives a graphical representation of the network health for the selected time period. The graphs can be viewed for the following time periods:

Last Week	Displays the report of the last seven days.
Last 24 Hours	Displays the report of the last 24 hours.
Last 15 Days	Displays the report of the last 15 days.
Last 30 Days	Displays the report of the last 30 days.

### Feature & Status

**Deployment Status:** Displays the number of clients deployed in the network as well as number of unprotected computers across your network. Click **Enumerate Now** to get up-to-date count of unprotected systems across your network.

**Client Status:** Displays the number of deployed clients, online clients, offline clients, and clients disconnected from the network.

**Update Status:** Displays the status of the clients updated till date, such as the number of clients updated, clients that have not been updated since three days, since the previous week, and since last fifteen days.

**Web Security:** Displays the blocked Web sites in a week. Top four categories are displayed in graphical representation and the rest of the categories are displayed as Others.

**Device Control:** Displays the number of devices such as CD/DVDs, configured USB devices, USB devices that have been blocked and the devices that have been denied write access in a week.

**Application Control:** Displays the status of all the applications blocked in a week. Top four categories are displayed in graphical representation and the rest of the categories are displayed as Others.

## Chapter 5. Clients

Clients includes features that help you manage and control all the clients deployed in the network. You can verify the current status of the clients and carry out various activities. You can scan client computers, update the software application, improve system performance, install and uninstall Quick Heal Endpoint Security Client remotely. You can also manage client groups, create and apply scanning policies and so on.

### Client Status

Client Status gives the current status of all the clients in the network. The status includes information such as the computer name, group name, domain name, IP and MAC addresses. It also shows protection status, installation status, product version, virus database date, last scan date, and protection polices among others.

To view Client Status, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Status**.
2. Under EPS Console, select a group name.  
*In the right pane, all the computers of a relevant group are displayed.*
3. Select a computer and then click **View Status**.

*The status of the selected computer appears. You can either export the status or take a print out if required.*

Show computers within subgroup	Helps you view computers that are in a subgroup.
View Status	Helps you view the status of the clients.
Remove Client	Helps you remove an offline client from a group.
Search	Helps you search the client by computer name.
CSV	Helps you save the report in CSV format.

### Client Action

Client Action allows you to scan computers remotely, update virus definitions, and improve performance of the computers. It also helps in verifying security compliance such as identifying unauthorized applications installed on any of the computers in the network.



The following table shows a comparison of the features in Client Action that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Scan	✓	✓	X
Update	✓	✓	✓
Tuneup	✓	X	X
Application Control Scan	✓	X	X

## Scan

This allows remote scanning of any computer in the network. A manual scan can be initiated with preconfigured policies. This reduces the additional task of personally overseeing each target computer.

To initiate scanning, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Action**.
2. Click **Scan**.

*A window displaying all the groups appears. Each group includes the names of computers belonging to that group.*

3. Under EPS Console, select a group.

*In the right pane, all the computers of a relevant group are displayed.*

4. To initiate scanning, click **Notify Start Scan**.

Show offline clients	Helps you view the computers that are not online or are disconnected from the network.
Show computers within subgroup	Helps you display the computers that are in a subgroup.
Scan Settings	Helps you customize scan settings.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Stop Notification	Helps you stop notification.

## Scan Settings

This feature allows you to customize the scan settings for a client machine.

To customize scanning, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Action > Scan**.
2. On the Scan screen, click **Scan Settings**.
3. On the Scan Settings screen, carry out the following:
  - i. Select either Quick Scan or Thorough Scan.  
*Quick Scan includes scanning of the drive where operating system is installed and Thorough Scan includes scanning of all fixed drives.*
  - ii. Select either Automatic or Advanced scan mode.  
*Automatic scanning involves optimum scanning and is selected by default.*
  - iii. Under **Select the items to scan**, select the files, file types (executable files, packed files, archive files), and mailboxes that you want to scan.
  - iv. In Archive Scan Level, set the scan level.  
*You can set the level for scanning in an archive file. The default scan level is 2. Increasing the default scan level may affect the scanning speed.*
  - v. In **Select action to be performed when virus found in archive file**, select an action.  
*The actions include: Delete, Quarantine, Skip. The action selected here will be taken automatically.*
  - vi. In **Select action to be performed when a virus is found**, select an action.  
*The actions include: Repair, Delete, Skip. The action selected here will be taken automatically.*
  - vii. Under Antimalware Scan Settings, select **Perform Antimalware scan** if required.
  - viii. In **Select action to be performed when malware found**, select an action.  
*The actions include: Clean and Skip. The action selected here will be taken automatically.*
4. After configuring the scan setting, click **Apply**.  
*The new setting is applied.*



Scan packed files, Scan mailboxes, and Antimalware Scan Settings are available only in the clients with Windows operating systems

## Update

This feature allows you to update the client applications on any computer in the network remotely. Quick Heal releases updates regularly to fix technical issues and provide protection against new threats. Hence, it is recommended that the protection software is updated regularly to the latest virus definitions.

To take the updates, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Action**.

2. Click **Update**.

*A window displaying all the groups appears. Each group includes the names of computers belonging to that group.*

3. Under EPS Console, select a group.

*In the right pane, all the computers of a relevant group are displayed.*

4. Select a computer and then click **Notify Update Now**.

*The selected computers are updated with latest virus definitions.*

5. To stop notification, click **Stop Notification**.

Select computers with out-of-date Quick Heal	Helps you update computers with outdated virus definitions.
Show computers within subgroup	Helps you display computers that are in a subgroup.
Notify Update Now	Helps you notify clients to update Quick Heal.
Stop Notification	Helps you stop notification.

## Tuneup

This facility improves the performance of the computers by defragmentation and by cleaning unwanted and junk files and invalid and obsolete registry entries. While you work in applications, computers write junks on the drives or when you visit Web sites, temporary files are created. Such junks and files occupy spaces in memory resulting in slowing down of the computers. Tuning up your computers cleans up such junks improving their performance.



- The Tuneup feature is available only in the clients with Windows operating systems.
- The Tuneup feature is not available for Windows Server operating system.

To tune up the computers, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Action**.

2. Click **Tuneup**.

*A window displaying all the groups appears. Each group includes the names of computers belonging to the group.*

3. Under EPS Console, select a group for which you want to perform Tuneup for.

*By default it shows all the computers present under EPS console.*

*In the right pane, all the computers of a relevant group are displayed.*

4. Select a computer and then click **Notify Start Tuneup**.

*Tuneup notifications are sent to the selected computers and Tuneup is performed on those computers.*

*You can stop Tuneup by clicking **Notify Stop Tuneup** or stop sending notification by clicking **Stop Notification** any time you prefer.*

Show offline clients	Helps you view the computers that are not online or are disconnected from the network.
Show computers within subgroup	Helps you display those computers that are in a subgroup.
Tuneup Settings	Helps you customize Tuneup settings.
Notify Start Tuneup	Helps you notify the clients to start Tuneup.
Notify Stop Tuneup	Helps you notify the clients to stop Tuneup.
Stop Notification	Helps you stop notification.

## Tuneup Settings

These settings allow you to carry out different types of cleanups such as disks, registry entries, or schedule a defragmentation at next boot.

To customize Tuneup settings, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Action > Tuneup**.

2. On the Tuneup screen, click the **Tuneup Settings** button.

3. On the Tuneup Settings popup, select any of the following:

- Disk Cleanup
- Registry Cleanup
- Defragment at next boot

*However, all these options are selected by default.*

4. To apply your settings, click **Apply**.

**Disk Cleanup:** Helps you find and remove invalid and unwanted junk files from the hard disk drive. These files consume hard disk space and also slow down the system considerably. Disk Cleanup deletes these files freeing up space that can be used for other applications and helps in improving system performance. This feature also deletes temporary files, Internet cache files, improper shortcut files, garbage name files and empty folders.

**Registry Cleanup:** Helps you remove invalid and obsolete registry entries from the system that appear due to improper uninstallation, non-existent fonts, and so on. Sometimes during uninstallation, the registry entries are not deleted. This leads to slower performance of the system. The Registry Cleanup removes such invalid registry entries to boost the performance of system.

**Defragment:** Helps you defragment vital files, such as page files and registry hives for improving the performance of the system. Files are often stored in fragments in different locations slowing down system performance. Defragment reduces the number of fragments and clubs all the fragments into one contiguous chunk to improve system performance.

## Application Control Scan

This allows you to check whether security compliance policies framed by your organization are being followed at each endpoint. It also helps you in verifying whether endpoints have any unauthorized applications other than the authorized ones running on them.



The Application Control Scan feature is available only in the clients with Windows operating systems.

To scan computers for compliance control, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Action**.
2. Click **Application Control Scan**.

*A window displaying all the groups appears. Each group includes the names of computers belonging to the group.*

3. Under EPS Console, select a group.

*In the right pane, all the computers of a relevant group are displayed.*

4. With the Scan Settings button, select your scan setting.
5. Select a computer and then click **Notify Start Scan**.

*The selected computers are scanned for compliance.*

*You can stop scanning by clicking **Notify Stop Scan** or stop sending notification by clicking **Stop Notification** any time you prefer.*

Show offline clients	Helps you view the computers that are not online or are disconnected from the network.
Show computers within subgroup	Helps display the computers that are in a subgroup.
Scan Settings	Helps you customize the scan settings for application control.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Stop Notification	Helps you stop notification.

## Scan Settings

This feature helps you customize your scan preference. To customize Scan Settings, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Action > Application Control Scan**.
2. On the Application Control Scan, click the Scan Settings button and then select any of the following:
  - Unauthorized applications: Helps you initiate scanning only for unauthorized applications present on a client machine.
  - Unauthorized and authorized applications: Helps you initiate scanning both for unauthorized and authorized applications present on a client machine.
  - All installed applications: Helps you initiate scanning for all applications installed on a client.

*You can select any one of the options for application control scan.  
Scanning by first two options may take time.*
3. To apply your settings, click **Apply**.

# Client Deployment

Client Deployment helps you synchronize with Active Directory groups to remotely deploy and install Quick Heal Endpoint Security Client on computers. It also compresses Quick Heal Endpoint Security Client setup and update files into a self-extracting file to simplify delivery through email, CD-ROM, or similar media. You can also enable login script setup to deploy Quick Heal Endpoint Security Client on remote systems when they log on to the selected domain or deploy Quick Heal Endpoint Security Clients through imaging. It also allows you to uninstall clients remotely.

The following table shows a comparison of the features in Client Deployment that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Through Active Directory	✓	X	X
Remote Install	✓	X	X
Notify Install	✓	✓	X
Client Packager	✓	X	X
Login Script	✓	X	X
Disk Imaging	✓	X	X
Remote Uninstall	✓	✓	✓

## Through Active Directory

This feature helps you sync with Active Directory groups. Once you sync the group, the clients will get installed on all the computers which come under your domain network. A periodic check is carried out to find if any new computer is added to your network. When a new computer is added, the client gets automatically installed on that computer.

You can also exclude certain computers from the Active Directory group so that the client is not installed on these computers.

Notes:

- This installation method is available only with Microsoft Windows operating system.
- To synchronize with Active Directory your console should be installed on the domain machine or should be a member of the domain.

- Synchronization cannot be done with 'Default' group.
- Groups shown in Red Color are already synched with Active Directory.
- The user should have permissions of “Domain Admins” to synchronize with Active Directory.
- The default synchronization time interval is GLOBAL.

## Synchronizing with Active Directory

To sync Active Directory groups, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Deployment**.
2. Click **Through Active Directory**.  
*A window appears with all the groups.*
3. Under EPS Console, select a group.  
*In the right pane, Active Directory Container and Synchronization Interval of the selected group are displayed, if already synched.*
4. Right-click a group and select Synchronize with Active Directory.  
*The Select a Domain screen appears.*
5. Select a domain and click **Next**.  
*The Authentication screen appears.*
6. Specify the user name in the format of "domain name\username" and enter a valid password and then click **Next**.  
*The Select Active Directory Container screen appears.*
7. Select Domain Name or Active Directory Container for Synchronization.  
*If you select a Domain Name, the whole Active Directory gets synched and if you select any Active Directory Container then only the selected container gets synched.*
8. Click **Next**.  
*The Synchronization screen appears.*
9. In Synchronization Interval, type the time interval when a periodic check is to be performed for this group and then click **Finish**.  
*Time should be specified between 1 to 24 hours.*  
*The directory is successfully synched.*

### Editing Synchronization

This feature gives you the flexibility to edit the time interval for carrying out periodic checks to find if a new computer is added to the network.

The frequency can be changed depending on how many and how often new computers are added.



To edit the time interval, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Deployment**.

2. Click **Through Active Directory**.

*A window appears with all the groups.*

3. Under EPS Console, right-click an already synced group and click **Edit Synchronization**.

*The authentication screen for Synchronization with Active Directory appears.*

4. Type the password and click **Next**.

*The Synchronization screen appears.*

5. In the Synchronization interval text box, type the time interval.

*Time should be specified between 1 to 24 hours.*

6. To save the new setting, click **Finish**.

*New synchronization setting is saved successfully.*

### **Removing Synchronization**

With this feature, you can remove the synchronization of a group in the following way:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Deployment**.

2. Click **Through Active Directory**.

*A window appears with all the groups.*

3. Under EPS Console, right-click a group that has already been synchronized and click **Remove Synchronization**.

*The synchronization of the selected group is removed successfully.*

### **Exclusion**

With this facility, selected workstations can be excluded from having the EPS Console client installed on them. You can exclude workstations by Host Name, IP Address or IP Range.

To exclude a workstation, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Deployment > Through Active Directory**.

2. On the Through Active Directory page, click the **Exclusion** button.

*A popup appears with the options about how you want to exclude a workstation.*

3. On the Exclude Workstations screen, select one of the following:

- **Exclude by Host Name:** If you select this option, type the Host Name and click **Add**. The workstation is added to the Excluded Workstations list.

- **Exclude by IP Address:** If you select this option, type the IP address and click **Add**. The workstation is added to the Excluded Workstations list.
  - **Exclude by IP Range:** If you select this option, type the Start IP Range and End IP Range details and click **Add**. The workstations are added to the Excluded Workstations list.
4. To save your settings, click **Save**.

Note: You can delete a workstation from the exclusion list whenever you prefer.

## Remote Install

This feature allows you to deploy the Quick Heal client on 2000 SP 4/ XP (Professional) / Server 2003 / Vista / Server 2008 / Windows 8/Server 2012 computers connected to the network. You can also install Quick Heal client on multiple computers at a time. Before proceeding with Remote Install, it is recommended that you go through the following requirements and changes:

### Exception Rules:

- On Windows Vista and later operating systems, Remote Installation is possible only with 'Built-in Administrator' account. To enable 'Built-in Administrator' account on computers running Windows Vista (or later), follow these steps:
  - Open Command Prompt in administrative mode.
  - Type 'net user administrator /active: yes' and press **Enter**.
  - Change the password of 'Built-in Administrator' from **Control Panel > User Accounts**.
- For remote installation of Endpoint Security Client on Windows XP Professional Edition, follow these steps:
  - Open My Computer.
  - Go to **Tools > Folder**.
  - Click the **View** tab.
  - Clear the option **Use simple file sharing**.
  - Click **Apply** and then click **OK**.
- Remote Installation of Quick Heal is not supported on Windows XP Home Edition. To install the Quick Heal client on Windows XP Home Edition, other methods of installation can be used, like Notify Install, Login Script, and Client Packager provided in Quick Heal Endpoint Security.
- Remote Install is not supported with the users having blank passwords on Windows XP and later operating systems.
- To install Quick Heal Client on systems which are under Domain Controller, specify the user name in 'DOMAINNAME\User Name' format

---

where DOMAINNAME is the name of the Domain Controller and User Name is the name of the Domain Administrator.

For Remote Install, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Deployment > Remote Install**.

*The Remote Install page opens.*

2. You can initiate remote installation in any one of the following ways:

- Remote Installation by Computers

- i. Under Network Places, select a computer, and then click **Add**. You can select multiple number of computers. You can also search a computer by the Find computer utility.

*Any computer in your network can be searched without enumerating the network.*

*For adding a computer you are required to provide the user credentials of the target computer, having administrator rights.*

- ii. On the Enter Network Password dialog, type the user credentials of the target computer and then click **OK**.

*Repeat these steps for all the computers that you have selected. .*

*If the entered user credentials are correct, the target computers appear in the **Computers selected to protect** list.*

*In case the user credentials to a computer are incorrect or you do not remember the user credentials to a computer, you can skip to the next computer and provide the user credentials to that computer by clicking the **Skip** button.*

- Remote Installation by IP Address

- i. Click the **Add by IP Address** button (you need not select any computer from the Network Places list)

- ii. On the Add Computer by IP Address dialog, select either of the following options:

- Add by IP Address Range: If you select this option, you must provide a range of IP Addresses in the Start IP Address option and the End IP Address option. This is helpful if you want to install the Quick Heal client on a number of computers which are available in serial IP Address range at one go.

- Add by IP Address: If you select this option, you need to provide the IP Address of the target computer.

- iii. Once you have entered the IP Address, click **Next**.

*For all the computers on which you want to install the client, you must provide the user credentials using the User Accounts option.*

- iv. For **User Accounts** under Add Computer by IP Address, click **Add**.

*The Add User dialog appears.*

- v. On the Add User dialog, type the user credentials and then click **OK**.

*Repeat this for all the computers on which you want to install the client.*

- vi. On the User Accounts list, click **Finish**.

*All the computers are added to the **Computers selected to protect** list.*

3. Click **Install**.

*Upon completion of the installation of the Quick Heal client agent, the installation status appears in the Result field of the selected computers list.*



The Remote Install feature is available only in the clients with Windows operating systems.

## Notify Install

This facility allows you to send email notification to the computers in the network to install the Quick Heal Endpoint Security client. The message can be typed and saved for future notifications. This can be edited whenever required.

To notify clients to install the Quick Heal client, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Deployment > Notify Install**.

*The Notify Install screen appears.*

2. In the **To** field, type the email address. In case of multiple recipients insert a semi colon (;) between email addresses.

*Modify the subject line of the message if necessary.*

3. Click **Send Notification**.

*The default email program on your system opens. Send the mail using the email program.*

Users have to click the link provided in the email that will redirect to the Quick Heal client installation Web page. The users need to install ActiveX and click **Install** to proceed with the Quick Heal client installation. After the Quick Heal client installation is finished, the Quick Heal AntiVirus installation will be initiated by the Quick Heal client.



The Notify Install feature is available only in the clients with Microsoft Windows and Mac operating systems.

---

## Client Packager

Client Packager can compress the Quick Heal client setup and update files into a self-extracting file to simplify delivery through email, CD-ROM, or similar media. It also includes an email function that can open your default email client and allow you to send the package from the Client Packager tool.

In Quick Heal Endpoint Security 5.2.1, Client packager can be created with or without the Quick Heal installer. The Client agent installer is helpful in situations where there are network bandwidth limitations to download the Quick Heal installer from the Endpoint Security server. . In such cases, you can create the Client agent installer including the Quick Heal installer and burn into a CD/DVD or copy it to a USB removable disk for deployment on endpoints.

When users receive the package, they just have to double-click the setup program to install. The Quick Heal clients installed through Client Packager communicates to the Quick Heal Endpoint Security server.

To create a Quick Heal Client package, follow these steps:

1. Go to **Start > Programs > Quick Heal EPS Console 5.2.1 > Client Packager**.
2. Select the Client Packager with or without the Quick Heal installer.
3. Select the setup type such as 32-bit or 64-bit according to your requirement.
4. Specify the folder path where you want to save Quick Heal Client Packager.
5. Click **Create**.



- The Client Packager feature is available only in the clients with Windows operating systems.
- To install Endpoint Security Client on 32-bit operating system, use 32-bit Client packager.
- To install Endpoint Security Client on 64-bit operating system, use 64-bit Client packager.

### ***Sending the package through email***

You need to have the default mail client installed to use the Client Packager email function.

To send the package from the console, follow these steps:

1. Click **Send mail**.

*The default email client will open. The email with the default subject and message appears. However, you can make changes to the subject and message, if required.*

2. In the **To** field, specify the recipients of this package.

*If required, you can also mark your email to other recipients in your organization in the Cc or Bcc recipients.*

3. Click **Send**.

## Login Script

### Installing Login Script

This feature allows you to assign a login script to the users so that they can deploy Quick Heal Client on remote systems when they log on to the selected domain. You can assign a script called QHEPS.BAT to the selected users in the domain. This script will install Quick Heal Endpoint Protection on the system when the user logs on to the concerned domain.



The Login Script feature is available only in the clients with Windows operating systems.

### Opening Login Script Setup

To open the Login Script Setup, follow these steps:

1. Select **Start > Programs > Quick Heal EPS Console 5.2.1**.
2. Click **Login Script Setup**.
3. Type the **Super Administrator Password** of Quick Heal Endpoint Security and click **OK**.

*The Login Script Setup application opens. The left panel of the application includes a tree-like structure that displays all the domains in your network.*

### Assigning Login Script

To assign Login Script, follow these steps:

1. Double-click the Domain.
2. Click the Domain Name.
3. Type the User Name and Password of the user having administrative privileges of the selected domain. A list of all users of the selected domain is displayed in the right panel.
  - i. Select a user or multiple users from the list to assign login script.
  - ii. To select all users, click **Check All**.
  - iii. To deselect all the selected users, click **Uncheck All**.
4. Select **Overwrite existing Login Script** if you want to overwrite the existing assigned login script of the selected users.
5. To assign login script to the selected users, click **Apply**.

*When a user logs on to the domain server, the assigned login script will deploy the Quick Heal client on the user system.*



- Users who do not have administrative privileges under the domain are shown in red color.
- The Result for a user can either be Assigned or Not Assigned. If the Result of a user is Assigned, it indicates that a script is assigned to that user. If the Result of a user is Not Assigned, it indicates that no scripts are assigned to that user.
- The Quick Heal client will get deployed only by the users having administrative privileges on Windows 2000 and later operating systems.

6. To exit the Login Script Setup application, click **Close**.

## Installing Quick Heal Endpoint Security on Mac Operating System

A Notify Install message containing a link for the installer file is sent from the administrator before installing Quick Heal Endpoint Security.

To install Quick Heal Endpoint Security, follow these steps:

1. Type the link in the browser.

*A web page appears that displays the prerequisites for installation and includes a link to the installer file (Download MAC Client). Please read the prerequisites carefully.*

2. Click through the **Download MAC Client** link.

*A tar file is downloaded that includes the installer.*

3. Go to the location where you have saved the tar file and extract all its components.

4. Double-click the installer file (**EPSMACCL.DMG**).

5. Run the Installer to start the Quick Heal Endpoint Security installation.

*Quick Heal Endpoint Security is installed successfully.*

## Installing Clients on Linux-based Systems

Quick Heal clients need to be manually installed by the Administrator on Linux-based systems.

To install the Quick Heal client on Linux-based systems, follow these steps:

1. For Linux-based client, copy the **aclinux** folder from the same system where the Quick Heal Endpoint Security server is installed. For example, if Quick Heal Endpoint Security is installed on C drive of the system, the **aclinux** folder would be available on the following path: **.\%ProgramFiles%\Quick Heal\Endpoint Security 5.2.1\Admin\web\build**.

2. Open the terminal on the Linux-based system.

3. Trace the path where the **aclinux** folder is saved.

4. Type the command **./install** to execute the installation script of Quick Heal.

*The installation script will do the following:*

- It copies the necessary files to /usr/lib/Quick Heal folder.
  - It will install Quick Heal client successfully.
5. This completes the Quick Heal client installation on Linux-based systems. At the command prompt, type **qhscanui** to open the Quick Heal scanner.

After installation:

- If Online Protection is not installed by ./install script, you can install online protection by running ./install script with --online parameter. If automatic installation of Dazuko fails, it prompts for the dazuko file. Quick Heal Online Protection (qhdaemon) requires Dazuko, a free software project providing access control. In order to use qhdaemon, you will need to compile Dazuko as kernel module or compile into the kernel. Visit <http://dazuko.org> for more details.
- Configure Quick Heal Online Protection. You can configure Quick Heal Online Protection later by running "configqhonline" from /usr/lib/QuickHeal/QuickHeal.

## Disk Imaging

You can deploy Endpoint Security client also through disk imaging like Sysprep. To deploy clients through Disk Imaging, follow these steps:

1. Disconnect the computer that will be used as a source for disk imaging from the network, or ensure that this computer is not able to communicate to the Endpoint Security server.
2. Install operating system and other applications.
3. Install Client. To install Client, follow these steps:
  - i. Create a Client Packager without AV Build, or
  - ii. Create a Client Packager with AV Build.
4. Create a disk image.

Note: All the Endpoint Security clients have GUID (Globally Unique Identifier). If the Endpoint Security client (after installation on the computer that is the source for disk imaging) communicates with the Endpoint Security server, the server will automatically assign GUID to this client. If such a client is Disk Imaged, then the Endpoint Security server will not be able to uniquely identify the clients after deployment of the image on multiple computers. To avoid this, ensure that the Endpoint Security client does not communicate with the Endpoint Security server when it gets installed on the computer that is the source for disk imaging.





The Disk Imaging feature is available only in the clients with Windows operating systems.

## Firewall Exception Rules

Operating systems such as Windows and Linux have their own Firewall bundled with them. If the user prefers to retain the firewall bundled with the Operating System, then exceptions can be created with Endpoint security for such systems. These exception rules are created during installation of Quick Heal Endpoint Security. For the system on which Quick Heal Endpoint Security is installed, the exceptions will be automatically created during installation. For the Quick Heal client the exception will automatically be created during deployment of Quick Heal clients.

The system with Quick Heal Endpoint Security will require three exception rules: one for the server, one for its own client, and one for the Endpoint Security site configured on it. The following are the exception rules for server:

- Agent Server 5.2
- Client Agent 5.2
- Endpoint Security Site Port 5.2

The system with the Quick Heal client will require one exception rule to be created. The following is the exception rule for clients:

- Client Agent 5.2

If the client system is a Linux-based system, the exception rule will be created in its Firewall as a port number.

## Remote Uninstall

With Remote Uninstall, you can remove the Quick Heal client along with AntiVirus program from the computers on your network remotely.



The Remote Uninstall feature is available in the clients with Microsoft Windows, Mac, and Linux operating systems.

To remove the client through Remote Uninstall, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Client Deployment > Remote Uninstall**.

*The Remote Uninstall dialogue appears that displays all the groups. Each group includes the name of computers belonging to the group.*

2. Select the computer from which you want to uninstall the Quick Heal client. To uninstall Quick Heal Client from all computers, click the checkboxes available to the computer name columns.

*You can also schedule uninstallation from computers that are not online or not present in the network by selecting **Show offline clients**. Select the Show Computers within subgroup to display the name of computers that are in the subgroup from the list of computers without actually exploring the network.*

3. Select **Start Uninstall Notification**.

*The uninstallation starts.*

### **Stop Uninstallation Notifications**

If you want to send notifications to stop uninstallation to the computers that have not yet started uninstallation, follow these steps:

1. Select the computers from which you want the clients should not be removed.
2. Click **Stop Uninstall Notification**.

*Clients that have not yet started the client uninstallation will skip the uninstallation request. However, clients that are already running the uninstallation program cannot stop the uninstallation procedure.*

Show offline clients	Helps you view the computers that are not online or are disconnected from the network.
Show computers within subgroup	Helps display the computers that are in a subgroup.

# Manage Groups

This feature helps you create groups and subgroups, and apply a policy to a group (or a subgroup). A group includes a number of clients and all the clients within a group share the same policy. You can delete or rename a group or set different policies for different group. You can also move clients from one group to another.

## Adding a Group

To add a new group, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Groups**.
2. Select the root node, for example Endpoint Security, and then right-click it.  
*A submenu appears with the options such as Add Group, Delete Group, Rename Group, Import from Active Directory, and Set Policy. However, only Add Group is enabled.*
3. Select **Add Group**.  
*The Add Group screen appears.*
4. In the Enter Group Name text box, type a group name.
5. Click **OK**.  
*The new group is added.*



No subgroup can be created under the Default group.

Show computers within subgroup	Helps you display the computers that are in a subgroup.
Search	Helps you search a computer name in a client.
CSV	Helps you save the report in CSV format.

## Adding a Subgroup

To add a subgroup, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Groups**.
2. Under EPS Console, select a group and then right-click it.  
*A submenu appears with the options such as Add Group, Delete Group, Rename Group, Import from Active Directory, and Set Policy.*
3. Select **Add Group**.  
*The Add Group screen appears.*

4. In the Enter Group Name text box, type a group name.
5. Click **OK**.

*The subgroup is added.*

### **Renaming a Group**

To rename a group, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Groups**.

2. Under EPS Console, select a group and then right-click it.

*A submenu appears with the options such as Add Group, Delete Group, Rename Group, Import from Active Directory, and Set Policy.*

3. Select **Rename Group**.

*The Rename Group screen appears. The old group name is also displayed.*

4. In the Enter New Name text box, type a new group name.
5. Click **OK**.

*The group name is modified. However, the policy applied earlier to this group does not change. To change a policy, you have to apply a new policy.*

### **Deleting a Group**

To delete a group, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Groups**.

2. Under EPS Console, select a group and then right-click it.

*A submenu appears with the options such as Add Group, Delete Group, Rename Group, Import from Active Directory, and Set Policy.*

3. Select **Delete Group**.

*A confirmation message is displayed.*

4. Click **OK**.

*The selected group is deleted.*

Note: If you delete a group that includes subgroups, then all the subgroups are also deleted.

## Setting Policy to a Group

Policies may include different client settings for different groups in an organization.

To set a policy to a group, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Groups**.

2. Under EPS Console, select a group and then right-click it.

*A submenu appears with the options such as Add Group, Delete Group, Rename Group, Import from Active Directory, and Set Policy.*

3. Click the **Set Policy** option.

*A list of policies appears.*

4. Select the policy that you want to apply.

*The policy is applied. The applied policy is displayed in the right panel along with the computer name, group, and other details.*

## Changing Group of a Client

This is helpful if you think a client should be in a certain group or the group has to be changed because of policy change at your organization. In case a change is incorporated, the protection policy of the new group will apply.

To change group of a client, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Groups**.

2. Under EPS Console, select a group.

*A list of all clients of the selected group is displayed in the right panel.*

3. Select a client and drag it to a different group where you want.

*The client is included in the new group.*

## Importing from Active Directory

This feature allows you to import Active Directory Structure in the console. This is helpful when you need to have group structure in the console that is already available in the Active Directory.

Note:

- To import from Active Directory, your Console must be installed on the domain machine or it should be a member of the domain.
- “Import From Active Directory” cannot be done with the default group.

To import Active Directory Structure, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and select **Clients > Manage Groups**.
2. Under EPS Console, right-click a group.  
*Add Group, Delete Group, Rename Group, Import from Active Directory, and Set Policy options are displayed.*
3. Select the **Import from Active Directory** option.  
*The Active Domain Controller dialog appears.*
4. Select a domain and then click **Next**.  
*The authentication screen appears.*
5. Type the user name in the format "domain name\user name" and then enter your password. Click **Next**.
6. On the Select Active Directory Container screen, select a Domain Name or Active Directory Container to import.
7. If you select a Domain Name, the whole Active Directory will get imported and if you select any Active Directory Container, only the selected container will get imported.
8. Click the **Finish** button.

# Manage Policies

Each organization prefers to enforce a policy that regulates its users. Quick Heal Endpoint Security allows the administrators to create policies that help centrally control and manage the users belonging to a group.

You can create a policy about permission to visit only certain Web sites, scan their systems regularly and implement policy for email communication. You can also restrict usage of certain applications and USB-based devices. . The Manage Policies feature gives you the flexibility and control over creating new policies and modifying or removing an existing policy. Different protection policies can be created for different groups for better control.

Policies may include different client settings and scan schedules. Once a policy is created, it can be easily applied to a group. The users under a group or a subgroup will inherit the same policy. A group is nothing but a department in an organization. You should create groups before you create a policy setting.

To learn about how to create a group, refer to [Adding a Group](#) in Chapter 7 “Manage Groups”, p - 46.

## Understanding Security Policy Scenario

The following example illustrates how different security policies can be created within an organization for different departments. Two departments namely Marketing and Accounts have been taken as an example.

Policy Settings for Marketing and Account Departments Compared			
Client Settings	Policy Features	Marketing Dept.	Accounts Dept.
Scan Settings	Scan mode	Automatic	Advanced
	Virus Protection Setting	Enabled	Enabled
	Block suspicious packed files	Enabled	Enabled
	Automatic Rogueware scan	Enabled	Enabled
	Disconnect Infected Clients Settings from the network	Not Enabled	Enabled

<b>Email Settings</b>	Email Protection	Enabled	Enabled
	Trusted Email Clients Protection	Enabled	Enabled
	Spam Protection Level	Soft	Strict
<b>External Drives Settings</b>	Scan External Drives	Enabled	Enabled
	Autorun Protection	Enabled	Enabled
	Mobile Scan	Not Enabled	Enabled
<b>IDS/IPS</b>	IDS/IPS	Enabled	Enabled
	Disconnect system from the network (only in case of DDOS and Port Scanning attack)	Not Enabled	Enabled
<b>Firewall</b>	Firewall	Enabled	Enabled
	Level	Low	High
<b>Web Security</b>	Browsing Protection	Enabled	Enabled
	Phishing Protection	Enabled	Enabled
Web Categories	Business	Allowed	Denied
	Social Networking	Denied	Denied
<b>Application Control</b>	CD/DVD Applications	Authorized	Unauthorized
	Games	Unauthorized	Unauthorized
<b>Device Control</b>	Removable Device Control	Enabled	Enabled
	Block complete access to removable devices	Not Enabled	Enabled
	Read only and no write access	Enabled	Not Enabled
<b>Update Setting</b>	Automatic update	Enabled	Enabled
	Download from Internet	Enabled	Not Enabled
	Download from Endpoint Security Console	Not Enabled	Enabled
<b>Internet Settings</b>	Proxy Settings	Enabled	Not Enabled
<b>General Settings</b>	Authorize access to the client settings	Enabled	Enabled



## Creating Policies

You can create different policies with different client settings and scan schedules to apply to different groups. This can help you manage the groups and users in a better way.

### **Creating a new policy**

To create a new policy, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Policies**.

2. To create a new policy, click **Add**.

*The new policy settings screen appears.*

3. In the Policy Name text box, type the policy name.

*After naming the new policy, you need to configure the client settings and schedule settings.*

4. To save your settings, click **Save Policy**.



While creating a new policy, you can allow the clients to configure their own settings by selecting the Let clients configure their own settings option.

### **Renaming a policy**

To rename a policy, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Policies**.

2. Click the policy that you want to rename.

*The selected policy appears with its settings*

3. In the Policy Name text box, rename the policy.

*You can change the policy settings also.*

4. To save your setting, click **Save Policy**.

### **Deleting a policy**

To delete a policy, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Policies**.

2. Select the policy that you want to delete, and then click **Delete**.

*A confirmation message appears.*

3. If you are sure to delete the selected policy, click **YES**.

*If the selected policy is applied to a group, it cannot be deleted and a message about **Failed to delete policies** appears.*



If a policy is applied to group and you want to delete it, apply a different policy to that group so the target policy is not applied to any group and then delete such a policy successfully.

## Importing and Exporting Policies

This feature allows you to import or export the policies of Quick Heal Endpoint Security. If you need re-installation or have multiple computers and want the same settings, you can simply export the settings configured on your current computer and easily import them on the computer(s). Both the default settings and the settings made by you can be exported.

Tip: The settings must be exported before you uninstall Quick Heal Endpoint Security. Importing or exporting the settings can be done in the same way.

### **Exporting a policy**

To export the policy settings, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Policies**.
2. Select a policy that you want to export and then click the **Export** button.
3. Select the drive and folder in which you want to store the policy.
4. Click **Save**.

*The policy settings file is exported to the selected location.*

### **Importing a policy**

To import the policy settings, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Clients > Manage Policies**.
2. Click the **Import** button.
3. Select the Import Settings file from the location where it exists.

*A new message appears that allows you to select which policies you want to import.*

4. Select the policies that you want to import and then click **Import**.

# Settings

This feature helps the administrators see and customize the settings of the default policy. The default policy is available as soon as you install the product on your system. The default policy includes both the client settings and schedule scan settings and is optimal for security that you can apply to a group. However, you can customize the settings according to the requirement but its name cannot be changed. The default policy is also available in the Manage Policies option (Quick Heal Endpoint Security > Clients > Manage Polices) from where you can customize its settings.

Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the Default button.

## Client Settings

### Scan Settings

This feature allows you to define a policy on how to initiate the scan of the client systems in your organization. The policy can be refined to enable Virus Protection or DNA scanning or include blocking of any suspicious packed files, and other settings.

The following table shows a comparison of the features in Scan Settings that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Automatic scan mode	✓	✓	X
Scan executable files	✓	✓	X
Scan all files (Takes longer time)	✓	✓	X
Scan packed files	✓	X	X
Scan mailboxes	✓	X	X
Scan archives files	✓	✓	X

To create a policy for Scan Settings, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then select **Settings**.
2. On the Settings screen, click **Scan Settings**.

- Under Scanner Settings, select the scan mode.

*The Scan Mode includes Automatic and Advanced.*

*You can enable Virus Protection, DNAScan, Block Suspicious files, Automatic Rogueware Scan, Disconnect Infected Client settings from the network, Exclude files and folders, and exclude extensions from being scanned.*

- To save your setting, click **Save Policy**.

## Scanner Settings

Under Scanner Settings, you can select either of the following scanning options:

- **Automatic:** This is the default scan setting that ensures optimum protection to the clients.
- **Advanced:** If you select this option, you may further need to customize the configuration of scanning options as per your requirement. When you select this option, other features are activated that are described as follows:

Features	Description
<b>Select items to scan</b>	Select either of the options to scan: <ul style="list-style-type: none"> <li>• Scan executable files: Includes scanning of executable files only.</li> <li>• Scan all files: Includes scanning of all files but takes longer time for scanning.</li> </ul>
<b>Scan Packed Files</b>	Scans packed files inside an executable file.
<b>Scan Mailboxes</b>	Scans emails inside the mailbox files.
<b>Scan Archive Files</b>	Scans compressed files such as ZIP and ARJ files including other files.
<b>Archive Scan Level</b>	You can set the level for scanning in an archive file. The default scan level is set to 2. You can increase the default scan level however that may affect the scanning speed.
<b>Select action to be performed when virus found in archive file</b>	You can select an action that you want to take when a virus is found in archive file during an on-demand scan. You can select any one of the following actions: <ul style="list-style-type: none"> <li>• Delete – Deletes the entire archive file even if a single file within the archive is infected.</li> <li>• Quarantine – Quarantines the archive containing the infected file(s).</li> <li>• Skip – Takes no action even if a virus is found in an archive file.</li> </ul>
<b>Select action to be performed when a virus is found</b>	You can select an action that you want to take when a virus is found during manual scan. You can select any one of the following actions: <ul style="list-style-type: none"> <li>• Repair – All the infected files are repaired automatically. The files that are not repairable are deleted.</li> <li>• Delete – All the infected files are deleted automatically.</li> <li>• Skip – Takes no action even if a virus is found in a file.</li> </ul>



To know for which clients the asterisked features are applicable, refer to the [comparison table](#) at page, 54.

## Virus Protection Settings

This feature helps you continuously monitor the client systems against viruses that may infiltrate from sources such as email attachments, Internet downloads, file transfer, and file execution. It is recommended that you always keep Virus Protection enabled to keep the client systems clean and secure from any potential threats.

The following table shows a comparison of the features in Virus Protection Settings that are applicable for different flavors of Quick Heal Endpoint Security clients:

Features	Clients		
	Windows	Mac	Linux
Load Virus Protection at Startup	✓	✓	✓
Display alert messages	✓	✓	X
Select action to be performed when a virus is found	✓	✓	X

With Virus Protection, you can configure the following:

Features	Description
Load Virus protection at Startup	Enables real-time protection to load every time the system is started.
Display Alert messages	Displays an alert message with virus name and file name, whenever any infected file is detected by the virus protection.
Select the action to be performed when a virus is found	<p>You can select an action that you want to take when a virus is found during manual scan. You can select any one of the following actions:</p> <ul style="list-style-type: none"> <li>• Repair – All the infected files are repaired automatically. The files that are not repairable are deleted.</li> <li>• Delete – All the infected files are deleted automatically.</li> <li>• Deny Access – Access to an infected file is blocked.</li> </ul>

## DNAScan Settings

Helps you safeguard the client systems even against new and unknown malwares whose signatures are not present in the virus definition database. DNAScan is an indigenous technology of Quick Heal to detect and eliminate such malicious threats in the system. DNAScan technology successfully traps suspected files with very less false alarms.

DNAScan Settings also includes the following:

Features	Description
Submit DNA suspicious files	Enables you to submit DNA suspicious files automatically.
Show notification while submitting files	Displays a notification while submitting DNA suspicious files.



The DNAScan Settings feature is available only in the clients with Windows operating systems.

### Block suspicious packed files

This feature helps you identify and block access to the suspicious packed files. Suspicious packed files are malicious programs that are compressed or packed and encrypted using a variety of methods. These files when unpacked can cause serious harm to the computer systems.

It is recommended that you always keep this option enabled to ensure that the clients do not access any suspicious files and thus prevent the spread of infection.



The Block suspicious packed files feature is available only in the clients with Windows operating systems.

### Automatic Rogueware Scan Settings

This feature automatically scans and removes rogueware and fake anti-virus software. If this feature is enabled, all the files are scanned for possible rogueware present in a file.



The Automatic Rogueware Scan feature is available only in the clients with Windows operating systems.

### Disconnect Infected Clients from the network

This disconnects the infected client(s) from the network. The following options are available:

**When non-repairable virus found:** Disconnects the client, if a non-repairable virus is found running in the memory.

**When suspicious file found by DNAScan:** Disconnects the client, if any suspicious file is found running in the memory.



The Disconnect Infected Clients from the network feature is available only in the clients with Windows operating systems.

## Exclude Files and Folders

This feature helps you decide which files and folders should be omitted from scanning for known viruses, DNAScan, and Suspicious Packed files. It is helpful in case you trust certain files and folders and want to exclude them from scanning.

The following table shows a comparison of the features in Exclude Files and Folders that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Exclude from: Known Virus Detection	✓	✓	X
Exclude from: DNAScan	✓	X	X
Exclude from: Suspicious Packed Files Scan	✓	X	X

To add a file or a folder, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **Scan Settings**.
3. Under Exclude File and Folders, click **Add**.
4. On the Exclude Item screen, select either of the following:
  - Exclude Folder: If you select Exclude Folder, type the folder path in **Enter folder path**.  
*If you want a subfolder also to be excluded from scanning, select **Include Subfolder**.*
  - Exclude File: If you select Exclude File, type the file path in **Enter file path**.
5. Select any one of the following as per your requirement:
  - Known Virus Detection
  - DNAScan
  - Suspicious Packed File Scan
6. To save your settings, click **OK**.

Important:

- If you select Known Virus Detection, DNAScan and Suspicious Packed File Scan will also be enforced and all the three options will be selected.
- If you select DNAScan, Suspicious Packed File Scan will also be enforced and both the options will be selected.

- However, you can select Suspicious Packed File Scan as a single option.

## Exclude Extensions

This feature helps you exclude the files from scanning by real-time virus protection by their extensions. This is helpful in troubleshooting performance related issues by excluding certain categories of files that may be causing the issue.

To exclude a file extension from scanning, follow these steps:

- Under Exclude Extensions, type an extension in the file extension name text box, and then click **Add**.

*The file extension should in the format: .xml, .html, .zip etc. without any dots.*



The Exclude Extensions feature is available only in the clients with Windows and Mac operating systems.

## Email Settings

This feature allows you to customize the protection rules for receiving emails from various sources. You can set rules for blocking spam, phishing and virus infected emails.

The following table shows a comparison of the features in Email Settings that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Enable Email Protection	✓	✓	X
Enable Trusted Email Clients Protection	✓	X	X

To configure Email Settings, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **Email Settings**.
3. Select the options that you want to enable.

*The Email Setting options include: Email Protection, Trusted Email Clients Protection, Spam Protection, Spam Protection Level, white list, and black list.*

4. To save your setting, click **Save Policy**.



---

## Email Protection

With this feature, you can apply the protection rules to all incoming emails. These rules include blocking infected attachments (malware, spam and viruses) in the emails.

To apply email protection to the users in a group, select Enable Email Protection. Once the feature is enabled, all incoming emails will be scanned before they are sent to Inbox.



The Email Protection feature is available only in the clients with Microsoft Windows and Mac operating systems.

## Trusted Email Clients Protection

Since email happens to be the most widely used medium of communication, it is used as a convenient mode to deliver malware and other threats. Virus authors always look for new methods to automatically execute their viral codes using the vulnerabilities of popular email clients. Worms also use their own SMTP engine routine to spread their infection.

Trusted Email Clients Protection is an advanced option that authenticates email-sending application on the system before it sends emails. This option prevents new 'worms' from spreading further. It includes a default email client list that is allowed to send emails. Email clients in the default list include Microsoft Outlook Express, Microsoft Outlook, Eudora, and Netscape Navigator.

Trusted Email Clients Protection supports most of the commonly used email clients such as Microsoft Outlook Express, Microsoft Outlook, Eudora and Netscape Navigator. If your email client is different from the ones mentioned, you can add such email clients in the trusted email client list.



The Trusted Email Clients Protection feature is available only in the clients with Windows operating systems.

## Spam Protection

This feature allows you to differentiate genuine emails and filter out unwanted email such as spam, phishing, and adult emails. We recommend you to always keep Spam Protection enabled. If you enable Spam Protection, the Spam Protection Level, White list, and Black list options are also activated.

The following table shows a comparison of the features in Spam Protection that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Spam Protection	✓	✓	X
Spam Protection Level	✓	X	X
Enable White list	✓	✓	X
Enable Black list	✓	✓	X

### Configuring Spam Protection

To configure Spam Protection, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, go to **Client Settings > Email Settings**.
3. Select **Enable Spam Protection**.
4. Under **Spam protection level**, set the protection level from the following:
  - **Soft**: Applies soft filtering spam protection policy.
  - **Moderate**: Ensures optimum filtering. It is recommended to have moderate filtering enabled. However, this is selected by default also.
  - **Strict**: Enforces strict filtering criteria. However, it is not ideal as it may block even genuine emails. Select strict filtering only if you receive too many junk emails
5. Select **Enable white list** to implement protection rules for whitelisted emails.
6. Select **Enable email black list** to implement the protection rules for blacklisted emails.
7. To save your settings, click **Save Policy**.



To know for which clients the asterisked features are applicable, refer to the [comparison table](#) at page, 61.

### **Setting spam protection rule for Whitelist**

Whitelist is the list of trusted email addresses. Content from the whitelisted email IDs is allowed to skip the spam protection filtering policy and is not tagged as SPAM.

This is helpful if you find that some genuine email IDs get detected as SPAM. Or if you have blacklisted a domain but want to receive emails from certain email addresses from that domain.

---

To add email addresses in the whitelist, follow these steps:

1. Select **Enable White List**.

*Check whether Spam Protection is enabled. If Spam Protection is enabled only then the whitelist option is activated.*

2. In the Email ID text box, type an email address or a domain and then click **Add**.

*You can import email addresses or domains from text file using the **Import** button.*

Note:

- An emails address should be in the format: [abc@abc.com](#).
- A domain name should be in the format: [\\*@mytest.com](#).



The same email ID cannot be entered in both Black List and White List.

### **Setting spam protection rule for Blacklist**

Blacklist is the list of email addresses from which all emails are filtered irrespective of their content. All the emails from the addresses listed here are tagged as "[SPAM] -".

This feature is useful particularly if your server uses an open mail relay, which is used to send and receive emails from unknown senders. This mailer system can be misused by spammers. With blacklist, you can filter incoming emails that you do not want or are from unknown senders both by email IDs and domains.

To add email addresses in the blacklist, follow these steps:

1. Select **Enable black List**.

*Check whether Spam Protection is enabled. If Spam Protection is enabled only then the blacklist option is activated.*

2. In the Email ID text box, type an email address or a domain and then click **Add**.

*You can import email addresses or domains from text file using the **Import** button.*

Note:

- An emails address should be in the format: [abc@abc.com](#).
- A domain name should be in the format: [\\*@mytest.com](#).



The same email ID cannot be entered in both Black List and White List.

## External Drives Settings

Whenever your system comes in contact with any external devices, your system is at risk that viruses and malwares may infiltrate through them. This feature allows you to set protection rules for external devices such as CDs, DVDs, and USB-based drives.

The following table shows a comparison of the features in External Drives Settings that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Scan External Drives	✓	X	X
Autorun Protection Settings	✓	X	X
Mobile Scan Settings	✓	X	X

To configure External Drives Settings, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **External Drives Settings**.
3. Select the options that you want to enable.  
*The External Drives Settings options include: External Drives Settings, Autorun Protection Settings, and Mobile Scan Settings.*
4. To save your setting, click **Save Policy**.

External Drives Settings includes the following:

### External Drives Settings

With External Drives Settings, you can scan the USB-based drives as soon as they are attached to your system. The USB-based drives should always be scanned for viruses before accessing it from your system, as these devices are convenient mediums for transfer of viruses and malwares from one system to another.

### Autorun Protection Settings

Autorun Protection protects your system from autorun malware that tries to sneak into the system from USB-based devices or CDs/DVDs using the autorun feature of the installed operating system.

---

## Mobile Scan Settings

This feature scans for viruses, spywares and other malwares in mobile devices. To scan your mobile device you need to connect it to PC using any of the following methods:

- USB Cable or
- Bluetooth.

Note: The Mobile Scan feature is not supported on server operating systems.

## IDS/IPS

When you create a network where numerous machines are deployed, security is of paramount concern. With IDS/IPS, you can detect attacks from various sources such as IDS/IPS, Port scanning attack, Distributed Denial of Service (DDOS) and so on. This detection implements a security layer to all communications and cordons your systems from unwanted intrusions or attack. You can also take actions like blocking the attackers for certain time, disconnecting the infected system from the network, and also send an alert message to the administrator.



The IDS/IPS feature is available only in the clients with Microsoft Windows.

You can create different policies with varying IDS/IPS settings and apply them to the groups so that each has separate policies based on the requirement.

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **IDS/IPS**.
3. Enable any of the following:
  - Enable IDS/IPS
  - Detect Port Scanning Attack
  - Detect DDOS(Distributed Denial of Service) Attack
4. From the following, select an action to be performed when attack is detected:
  - Block Attackers IP for ... Minutes.  
*Enter time here.*
  - Disconnect system from the network (only in case of DDOS and Port Scanning attack).
  - Display alert message when attack is detected.  
*This helps you take an appropriate action when attack is detected.*
5. To save your setting, click **Save Policy**.

---

### **Customization for Port Scanning**

Further customization settings for Detect Port Scanning Attack and Detect DDOS (Distributed Denial of Service) Attack are as follows:

1. On the IDS/IPS screen, click **Customize** available next to Detect Port Scanning Attack or Detect DDOS (Distributed Denial of Service) Attack.  
*A dialogue for further settings appears.*
2. Select one of the levels from:
  - Soft: Detects attack if many ports are scanned.
  - Normal: Detects attack if multiple ports are scanned.
  - Strict: Detects attack even if a single port is scanned.
  - Custom: Helps you customize the attack condition and number of scanned ports exceeds than field.
3. To exclude an IP address that you do not want to be scanned, click **Add** under Excluded IP Addresses.
4. On the Add IP Address screen, type an IP Address or IP range and then click **OK**.
5. To exclude Port that you do not want to be scanned, click **Add** available under Excluded Ports.
6. On the Add Port screen, type a Port or Port range and then click **OK**.

### **Customization for Distributed Denial of Service**

Further customization settings for Distributed Denial of Service Attack are as follows:

1. On the IDS/IPS screen, click **Customize** available next to Detect DDOS (Distributed Denial of Service) Attack.  
*A dialogue for further settings appears.*
2. Select one of the levels from:
  - Soft: Detects if many attacks occur.
  - Normal: Detects if multiple attacks occur.
  - Strict: Detects attack even if a single attack occurs.
  - Custom: Helps you customize the attack condition and number of attack sources exceeds than the specified limits.
3. To exclude an IP address that you do not want to be scanned, click **Add** under Excluded IP Addresses.
4. On the Add IP Address screen, type an IP Address or IP range and then click **OK**.
5. To exclude Port that you do not want to be scanned, click **Add** option available under Excluded Ports.

6. On the Add Port screen, type a Port or Port range and then click **OK**.

## Firewall

Firewall shields your system by monitoring both inbound and outbound network traffic. It analyzes all incoming traffic whether it is secure and should be allowed through, and checks whether the outgoing communication follows the compliance that you have set for security policies. Firewall works silently in the background and monitors network activity for malicious behavior.

You can create different policies for various groups/departments like enabling Firewall protection, applying Firewall security level with an exception rule and other settings according to the requirements. For example, you can apply security level as High for the Accounts Department, and apply an exception rule by entering the policy with additional policy settings. You can also apply the *Display alert message when firewall violation occurs* and *Enable firewall reports* options. While for Marketing Department, you can create a policy with security level as Low without an exception rule and apply the *Enable firewall reports* options only.



The Firewall feature is available only in the clients with Microsoft Windows.

To configure a policy for Firewall setting, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **Firewall**.
3. To enable Firewall, select **Enable Firewall**.
4. In the Level option, select one of the following:
  - Block all
  - High
  - Medium
  - Low
5. If you want an alert message about firewall violation, select **Display alert message when firewall violation occurs**.
6. If you want reports for all blocked connections, select **Enable firewall reports**.
7. To save your setting, click **Save Policy**.

Note: If the Firewall policy is set as 'Block All' or 'High', Firewall will block all connections and generate many reports that may impact your network traffic.

### Exceptions

Security Level	Description
Block all	Blocks all Inbound and Outbound traffic without any exception. This is the strictest level of security.
High	Blocks all Inbound and Outbound traffic with an exception rule. The exception policy can be created for allowing or denying traffic either for inbound or outbound through certain communication Protocols, IP address, Ports such as TCP, UDP, ICMP.
Medium	<p>Blocks all Inbound and allows all Outbound traffic with an exception rule.</p> <p>The exception policy can be created for allowing or denying traffic either for inbound or outbound through certain communication Protocols, IP address, Ports such as TCP, UDP, ICMP. For example, if you allow to receive data from a certain IP address, the users can receive data but cannot send to the same IP address.</p> <p>To take more advantage of this security level policy, it is advisable that you allow to receive inbound traffic and block outbound traffic.</p>
Low	<p>Allows all Inbound and Outbound traffic.</p> <p>When you apply Low security level, it is advisable that you create an exception rule for denying particular inbound or outbound data with the help of certain Protocols, IP address, and Ports to take more advantage of the security level policy.</p>

### Exceptions

With exceptions, you can allow genuine programs to perform communication irrespective of Firewall level set as High or Medium. You can add exception to allow inbound and outbound communication through IP Addresses and Ports. With Exceptions, you can block or allow Inbound and Outbound communication, through IP Addresses and Ports.

To configure a policy with the Exceptions rule, follow these steps:

1. Under Exceptions, click **Add**.
2. On the Add/Edit Exception screen, type a name in the Exception Name text box and select a protocol. Click **Next**.

*The protocol includes: TCP, UDP, and ICMP.*

3. Select a direction for traffic and then click **Next**.

*Traffic direction includes: Inbound and Outbound.*

If you select Outbound, the setting applies only to the Outbound traffic. If you select both Inbound and Outbound, the setting applies to both types of traffic.

4. Under IP Address, type an IP address or IP range and then click **Next**.

*If you select Any IP Addresses, you need not type an IP address as all IP addresses will be blocked.*

5. Under TCP/UDP Ports, type a port or port range and then click **Next**.

*If you select All Ports, you need not type a port as all ports are selected.*



6. Under Action, select either **Allow** or **Deny**. Click **Finish**.

## Web Security

This feature helps you create security policies for a department or group where Browsing and Phishing Protection can be enabled. This blocks malicious and phishing web sites. You can also restrict or allow access to the websites as per your requirement.

The following table shows a comparison of the features in Web Security that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Browsing Protection	✓	✓	X
Phishing Protection	✓	✓	X
Restrict access to particular categories of Websites (Web Categories)	✓	✓	X
Block specified websites	✓	✓	X

To create a policy for Web Security, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **Web Security**.
3. Under Web Security, select either of the following or both:
  - Browsing Protection
  - Phishing Protection
4. To save your setting, click **Save Policy**.

### Browsing Protection Settings

While users visit malicious websites some files may get installed on their systems. These files can spread malware, slow down the system, or corrupt other files. These attacks can cause substantial harm to the system.

Browsing Protection ensures that malicious websites are blocked while the users in a group are accessing the Internet. Once the feature is enabled, any site that is accessed is scanned and blocked if found to be malicious.

## Phishing Protection Settings

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. These emails usually appear to have been sent from seemingly well-known organizations and sites such as banks, companies and services seeking for your personal information such as credit card number, social security number, account number or password.

Administrators can enable Phishing Protection that prevents users from accessing phishing and fraudulent websites. As soon as a site is accessed, it is scanned for any phishing behavior. If found so, then it is blocked to prevent any phishing attempts.

### **Exclusion for Browsing Protection and Phishing Protection**

Exclusion enables you to apply an exception rule to the protection policy for Browsing Protection and Phishing Protection. This helps you exclude the URLs of the sites that are actually genuine but get erroneously detected either as malicious or phishing sites. You are recommended to exclude only those URLs that you trust to be safe and genuine.

You can exclude the URLs in the following way:

1. On the Web Security screen, click the **Exclusion** button.

*The Exclude URLs dialogue appears.*

2. In the Enter URL text box, type the URL and then click **Add**.

*The Report Miscategorized URL dialogue appears. You can report about miscategorization of the URL to the Quick Heal lab if it gets detected either as malicious or a phishing site.*

3. Select one of the reasons from the following:

- URL is getting detected as Malicious.
- URL is getting detected as Phish.

4. To report about miscategorization, click **Yes**. If you do not want to report about miscategorization, click **No**.

*The URL is added in the Exclude URL list.*

5. To save your settings, click **OK**.

Add	Helps you exclude a URL from being detected as malicious or phishing.
Delete	Helps you delete a URL from the Excluded URL list.
Report	Helps you report if a URL is miscategorized.

## Web Categories

There are certain concerns that most organizations may face:

- System infection by malware.
- Users browsing unwanted websites.
- The employees idling away time.

To avoid these concerns the administrators need to have a policy that regulates users and their web access activities.

The Web Categories feature helps the administrators centrally control and manage the browsing behavior of the users. The administrators can create different security policies for different groups according to their requirements and priorities.



The Web Categories feature is available only in the clients with Microsoft Windows and Mac operating systems.

To configure Web Categories, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **Web Security**.
3. Under Web Categories, select **Restrict access to particular categories of Websites**.

*The web categories are enabled and you can allow or deny access to each category.*

4. Under Status to each category, select either **Allow** or **Deny**.

### Exclusion for Web Categories

Exclusion helps you apply an exception rule to the protection policy for Web Categories. This helps you when you want to restrict access to a website category but you want to allow certain websites from the restricted category.

You can enlist such websites in the Exclusion list in the following way:

1. Under the Web Categories screen, click the **Exclusion** button.

*The Exclude URLs dialogue appears.*

2. In the Enter URL text box, type the URL and then click **Add**.

*The URL is added in the Exclude URL list.*

3. To save your setting, click **OK**.

Add	Helps you exclude a URL from being restricted even if it belongs to the blocked category.
Delete	Helps you delete a URL from the Excluded URL list.

### **Block specified websites**

This feature is helpful in restricting access to certain websites or when a website does not fall into an appropriate category. It is also helpful if you have a shorter list of the websites that you would prefer to restrict the websites than blocking the entire category.

To block websites, follow these steps:

1. On the Web Security screen, select **Restrict access to particular Websites** under Block specified websites.

*The Block specified websites features (Add, Delete, Delete All) are activated.*

2. To add a website, click **Add**.

3. On the Add URL screen, type a URL in the **Enter URL** text box.

*If you want to block subdomain select **Also Block Subdomains**. For example, if you block [www.google.com](http://www.google.com) and select 'Also block subdomains', all its subdomains such as [mail.google.com](http://mail.google.com) will also be blocked.*

4. To save your setting, click **OK**.



- The Block specified websites feature is available only in the clients with Microsoft Windows and Mac operating systems.
- The Also Block Subdomains feature is not applicable for the clients with Mac operating systems.

### **Application Control**

Organizations usually face the following concerns while using applications:

- No illegal or fake applications should be installed on client systems.
- Malicious applications should not infect the systems.
- Unnecessary applications should not clog the systems.

With this feature, the administrators can authorize or unauthorize the users to access and work with certain applications, so that no one accesses an unwanted application. If the users try to access an unauthorized application, a notification can also be sent to the users about why they cannot access the application.

The administrators can create various policies based on the requirement of the groups or departments. For example, for the users of the Marketing Dept., you can allow access to File Sharing Applications and Web Browser while restrict access to all other applications. For the Accounts Dept., you can allow access to Archive Tools and Web Browsers only.



- The Application Control feature is available only in the clients with Windows operating systems.

---

To create a policy for Application Control, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **Application Control**.
3. To block access to an application, select **Block unauthorized application when accessed**.
4. If you want to send a notification when a blocked application is accessed, select **Notify clients when an unauthorized application is blocked**.
5. Select either Authorized or Unauthorized to each application category as per your requirement.

*You can also customize the setting to the application category by clicking the Custom button.*

6. To save your setting, click **Save Policy**.

### **Custom**

You can customize the application settings that would authorize or unauthorize specific applications or categories. If you authorize or unauthorize an application category, all the applications listed under that category are either allowed or blocked.

For example, from the application category 'Email Clients', you can unauthorize access to 'Thunderbird', and 'MailWasher' and authorize access to all the other applications. Similarly, for the application version 'Thunderbird', you can unauthorize access to 'Thunderbird 1' and authorize access to all the other versions of that application.

You can customize the applications in the following way:

1. Under Application Control, click **Custom** to an application category.  
*Ensure that the option **Block unauthorized application when accessed** is selected, only then you can click the Custom option.*  
*A list of applications under the selected application category appears.*
2. In the list of applications, select all application names that you want to unauthorize and leave out those that you want to authorize.
3. To save your setting, click **Save Policy**.

### **Add Application**

This feature allows you to add a new application to the default list. Adding and unauthorizing of an application or file that belongs to the operating system or other system specific aspects may cause system malfunction. Hence it is advised to add an application that is not a part of operating system or other system related programs.

You can add an application in the following way:

1. On the Application Control screen, click the **Custom Applications** button under Add Application.
2. On the Custom Applications screen, click **Add Application**.
3. Browse and give the path to the application.
4. In the Application Name text box, type an application name.
5. In the Application Category list, select a category.

*You can also write a reason for adding a new application to the default list of applications. This helps Quick Heal to improve the quality of the software product.*

*You can also submit the application metadata to the Quick Heal lab.*

6. To add the application, click **Add Application**.

### **Submit Application metadata to Quick Heal Lab**

With this option, you can send metadata of an application to the Quick Heal lab for including it in the application categories. Metadata includes information of application such as its Name, Version, Company Name, MD5. You can also provide the reason for adding the application. This information will help us to improve the Application Control module.

Application Categories include thousands of applications based on their functionalities. If you block a category, all the applications in that category are blocked.

However, if you have unauthorized an application category but an application is not yet blocked, you can submit that application. Quick Heal analyzes the application and then enlists it in the category.

Note:

- User may get application blocked prompt even while copying or renaming any unauthorized application.
- Some unauthorized applications may start in case the application executable is updated due to software update. Such applications can be added to Endpoint Security Console and you are recommended to submit the Metadata to the Quick Heal lab.

## **Device Control**

While working with data storage devices such as CD/DVDs and USB-based devices such as pen drives, organizations are concerned with the following:

- Client systems are clean and no malware is installed on them.
- Autorun feature does not activate any infection.
- Unnecessary data or applications do not clog the systems.

This feature allows the administrators to create policies with varying rights. For example, administrators can block complete access to removable devices, give Read only and no write access so that nothing can be written on the external devices. They can also customize access to admin configured devices. Once the policy is applied to a group, the access rights are also applied.



The Device Control feature is available only in the clients with Windows operating systems.

To create a policy for Device Control, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **Device Control**.  
*A list of all removable devices, if you have added any, appears in the list.*
3. To enable removable device control, select **Enable Removable Device Control**.
4. Under Select policy for removable devices, select one of the following as per your requirement:
  - Block complete access to removable devices
  - Read only and no write access
  - Customize access to admin configured devices

If you select Customize access to admin configured devices, *Allow read only access to other USB storage devices* and *Allow complete access to CD/DVD drives* options get activated that you can select as required.

*You can customize the access policy to the individual devices by selecting different rights (Block Access, Read Only Access, Full Access) available next to each device.*
5. To save your setting, click **Save Policy**.

*This policy is applied to all the removable devices in the list. Even if you add a device later the same policy will apply unless you customize the policy.*

Note:

- The Customized Access option of Device Control is not supported on Quick Heal Endpoint Security 5.2.1 Client if installed on Windows 2000 family, Windows XP Service Pack 1 and previous, and Windows 2003 without Service Pack. Hence, encrypted devices will not be accessible on these operating systems.
- Only formatted USB Pen Drives with NTFS File System can be added for authorization.
- USB Pen Drives with GUID Partition Table (GPT) Partition Style cannot be added for authorization.

- If an authorized and encrypted device is formatted, the device will be treated as unauthorized. Hence, Administrator will need to add the device again in Device Control and configure the policies accordingly.

### **Adding Device to Server**

To know about how to add a device to the server, refer to [Add Device](#) in Chapter 10, “Admin Settings”, p - 87.

## **Update Settings**

When a work environment has a large number of systems installed, the challenge that the administrators usually face is how to update all the client systems for security patches.

This feature allows you to create policies for taking the updates automatically for the clients. You can create policies that help different clients take the updates from different sources. Taking the updates from different sources reduce the load on a single server.

The following table shows a comparison of the features in Update Settings that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Enable Automatic Update	✓	✓	✓
Show update notification window	✓	✓	X
Frequency	✓	✓	X
Update Mode	✓	✓	✓

To create a policy for Update Settings, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **Update Settings**.
3. To take the updates automatically, select **Enable Automatic Update**.
4. To display notification window when the updates are taken, select **Show update notification window**.
5. Under Frequency, set the schedule when you want to take the updates.
  - Automatic
  - As per schedule

If you select As per schedule, *Daily Start time* and *Repeat after* are activated that you can set as per requirement.



6. To set how to take the updates, select one of the following options under Update Mode:
  - Download from Internet
  - Download from Endpoint Security Console
  - Download from Specified Update ServersFor creating different policies, you can select different options for Update Mode.  
If you select Download from Specified Update Servers, you should enter the update server locations in the list.
7. To save your settings, click **Save Policy**.

Note: If you select the option Download from Specified Update Servers, the Linux client will download the updates from the Endpoint Security server.



To know for which clients the asterisked features are applicable, refer to the [comparison table](#) at page, 75.

### ***Entering update server locations***

If you select the **Download from Specified Updates Servers** option, you are advised to enter the update server location to take the updates. In case of large networks, you can also deploy multiple Update Managers. This helps load balancing as the clients can take the updates from different servers. If you have configured multiple Update Managers in your network, specify their URLs in this section. You can configure clients to take the updates from these locations in Client Settings.

To enter a server location, follow these steps:

1. On the Quick Heal Endpoint Security Dashboard, click **Home**.
2. On the Home page, click the **Update Manager** link, available next to the product name and version details.
3. On the Update Manager screen, click **Alternate Update Managers**.
4. In the Enter Update Manager URL text box, type a URL and then click **Add**.

*You can arrange the URLs according to your priority. The URLs added will be available in the update server location list in **Update Settings**.*

### **Internet Settings**

This feature gives the administrators a wider choice of creating policies for the client modules that need Internet connection to function. You can configure different settings for the server and port so that the client modules such as Quick Update, Spam Protection, Web Security, and Messenger have Internet connection.

This is very helpful in allowing the client modules to function in a secure work environment where default Internet connection is not allowed.

To create a policy with Internet Settings, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **Internet Settings**.
3. To set the proxy setting for Internet, select **Enable Proxy Setting**.  
*The proxy settings details are activated.*
4. In Proxy Type, select the proxy type that you need for Internet connection.  
*Proxy types include: HTTP Proxy, SOCKS V4, and SOCKS V5.*
5. In Proxy Server, type the sever name.
6. In Port, type the port number.  
*You can also set authentication rule if you use Firewall or proxy server. For this, type the User name and Password under Authentication.*
7. To save your setting, click **Save Policy**.



The Internet Settings feature is applicable for the clients such as Microsoft Windows, Mac, and Linux operating systems.

## General Settings

This feature allows you to create a policy that authorizes the clients to access client settings and change their own password, enable or disable Self Protection and news alert.

The following table shows a comparison of the features in General Settings that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Authorize access to the client settings	✓	✓	X
Enable Self Protection	✓	X	X
Enable News Alert	✓	X	X

To create a policy for General Settings, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **General Settings**.

- To give access to the client settings, select **Authorize access to the client settings**.

*Password setting is activated.*

- In Enter Password, type the password and then re-type the same password in Confirm Password.

*The clients will have to use these passwords for accessing the client settings.*

- To activate Self Protection, select **Enable Self Protection**.
- To get the news alert about various incidents, select **Enable News alert**.
- To save your setting, click **Save Policy**.



To know for which clients the asterisked features are applicable, refer to the [comparison table](#) at page, 77.

## Schedule Settings

Scanning regularly keeps the systems clean and safe. In a large organization the client systems may be installed in physically separated environments.

To centrally manage all the systems about how to scan and when to initiate scanning, the administrator must have a policy. This feature helps you create policies for scheduling scans for the client systems.

You can schedule scanning for the following.

### Client Scan

This feature allows you to create policies to initiate scanning the clients automatically at a convenient time. You can define whether the scan should run daily or weekly, select scan mode (Quick Scan, Thorough Scan). You can also enable Antimalware while scanning. This will supplement other automatic protection features to ensure that the client systems remain malware-free.

The following table shows a comparison of the features in Client Scan that are applicable for different Quick Heal Endpoint Security clients on different operating systems:

Features	Clients		
	Windows	Mac	Linux
Client Schedule Scan	✓	✓	X
Antimalware Scan Settings	✓	X	X

---

To create a scan schedule policy for Client Scan, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, go to **Schedule Settings > Client Scan**.
3. Configure the following settings: Client Schedule Scan, Scanner Settings, and Antimalware Scan Settings.
4. To save your settings, click **Save Policy**.

Note: You can revert to the default settings whenever you prefer by clicking the Default button.

### **Client Schedule Scan**

This feature helps you define scan schedules for the clients at a certain frequency. To configure Client Schedule Scan, follow these steps:

1. Under Client Schedule Scan, select **Enable Schedule Scan**.
2. In Frequency, select either the **Daily** or **Weekly** option.
3. In **Start At**, set time in hours and minutes.
4. If you want to repeat scanning of your clients, select **Repeat Scan** and set the frequency after what interval the scan should be repeated.
5. To get notification when a client is offline, select **Notify if client is off-line**.

### **Scanner Settings**

This feature helps you define what scan mode you prefer for scanning the clients or what items you want to scan.

To configure Scanner Settings, follow these steps:

1. Under How to Scan, select a scan mode from the following:
  - Quick Scan (Scan Drive where operating system is installed)
  - Thorough Scan (Scan all the fixed drives).
2. To set optimal setting, select the **Automatic** option.
3. To set advanced setting, select the **Advanced** option.

*If you select the Advanced option, further settings such as scan items and scan types are activated.*

4. Under Select items to scan, select any of the following:
  - Scan executable files
  - Scan all files (Takes longer time)
  - Scan packed files

- Scan mailboxes
  - Scan archives files
5. If you select the Scan archives files option, you can set the following also:
    - Archive Scan Level: You can set up to level 5.
    - Select action to be performed when virus is found in archive file: You can select one of the actions from Delete, Quarantine, Skip.
  6. In Select action to be performed when a virus is found, select an action from the following: Repair, Delete, Skip.

### **Antimalware Scan Settings**

This feature helps you enable scanning for malware. To configure Antimalware Scan Settings, follow these steps:

1. To enable scanning for malware, select **Perform Antimalware scan**.
2. In **Select action to be performed when malware found**, select an action from the following: Clean and Skip.



Scan packed files, Scan mailboxes, and Antimalware Scan Settings are available only in the clients with Windows operating system.

### **Application Control**

This feature allows you to create policies to initiate scanning of the applications installed on the clients automatically at a convenient time. It also helps you scan all authorized and unauthorized applications present on the clients.

To create a policy for scanning applications, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, go to **Schedule Settings > Application Control**.
3. Configure the following settings: Application Control Schedule Scan and Scan and Report.
4. To save your setting, click **Save Policy**.

Note: You can revert to the default settings whenever you prefer by clicking the Default button.



The Application Control Schedule Scan feature is available only in the clients with Windows operating systems.

---

### ***Application Control Schedule Scan***

This feature helps you define schedules to scan applications at a preferred or specified frequency. To configure Application Control Schedule Scan, follow these steps:

1. Under Application Control Schedule Scan, select **Enable Schedule Scan**.
2. In Frequency, select either the **Daily** or **Weekly** option.
3. In **Start At**, set time in hours and minutes.
4. If you want to repeat scanning for the applications, select **Repeat Scan** and set the frequency of interval after which the scan should be repeated.
5. To get notification when a client is offline, select **Notify if client is off-line**.

### ***Scan and Report***

This feature allows you to initiate scanning of the applications in various ways.

Under Scan and Report, select one of the following options:

- Unauthorized applications
- Unauthorized and authorized applications
- All installed applications

### **Tuneup**

This feature helps you create policies to tune up the clients automatically at preferred time and intervals.

To create a policy for Tuneup, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, go to **Schedule Settings > Tuneup**.
3. Configure the following settings: Tuneup Schedule Scan and Tuneup Settings.
4. To save your setting, click **Save Policy**.

Note: You can revert to the default settings whenever you prefer by clicking the Default button.



The Tuneup Schedule Scan feature is available only in the clients with Windows Desktop operating systems.

### ***Tuneup Schedule Scan***

This feature helps you define schedules to tune up the clients at the preferred frequency. To configure Tuneup Schedule Scan, follow these steps:

1. Under Tuneup Schedule Scan, select **Enable Schedule Scan**.
2. In Weekday, select a day of the week.
3. In **Start At**, set time in hours and minutes.
4. If you want to repeat scanning, select **Repeat Scan** and set the frequency after what interval the scan should be repeated.
5. To get notification when a client is offline, select **Notify if client is off-line**.

### ***Tuneup Settings***

This feature helps you define how the tuneup process should run and what should be cleaned. You can select either or all of the following options:

- Disk cleanup
- Registry cleanup
- Defragment at next boot

## Chapter 10. **Admin Settings**

### **Server**

This feature allows you to configure various settings related to sever. This includes settings on how to send notifications and for what reasons, SMTP settings, and adding devices to allow access, redirecting server in case of need, and managing users.

#### **Password**

To prevent unauthorized users from modifying your settings or removing the Quick Heal client from computers it is advisable that you password-protect Quick Heal Endpoint Security. Quick Heal Endpoint Security requires you to specify a console password; however, you can modify your password from the Quick Heal Endpoint Security.

To change the console password, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > Change Password**.
3. In the Old Password text box, type current Super Administrator Password.
4. In the New Password text box, type the new password, and then re-type the new password in the Confirm Password text box.
5. Click **Apply**.

#### **Notification**

This feature helps you set rules for sending notifications for various events such as when virus is detected, virus is active in memory, or there is a virus outbreak. Notifications are sent against intrusion detection, if an unauthorized device or application is accessed or virus definitions get outdated. This also includes alerts for failure of synchronization with Active Directory, or any license related information etc. Notifications keep you informed about the incidents occurring across the network so that appropriate action can be taken to avoid any mishap.

Notification includes the following:

- Email & SMS Notification – for notification for various incidents.
- Configure Email & SMS for Event Notification – for creating a list of Email IDs and Mobile Numbers for sending SMS.



### **Email & SMS Notification**

To configure Email & SMS Notification, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > Notification**.
3. To activate notifications to be sent, select the **Select Event for which notification should be sent** option under Email & SMS Notification.

*All other options under Notifications to be sent are activated.*

4. Under **Virus Infection and Virus Outbreak**, select the mediums through which you want to get the notification for the following incidents:
  - Virus detected on clients
  - Virus active on client
  - Virus outbreak in network

*You can get notifications either through Email or SMS or both. However, for Virus detected on clients, you can get the notification only through email.*

*If you select the option Virus outbreak in network, you can further customize the settings on when you want the notifications. This alerts you on virus outbreaks.*

To customize Virus outbreak in network, follow these steps:

- Next to Virus outbreak in network, click **Customize**.  
*The Virus Outbreak details screen appears.*
  - Under **Total number of virus incidents exceeds**, set number of incidents and the number of systems on which the virus outbreak happens.
  - Under **And in the time span of**, set time about how often the notification will be triggered.
  - To save your setting, click **Save**.
5. Under **Intrusion Prevention**, select the mediums through which you want to get notification for the following incidents:
    - Intrusion detected on client
    - Port Scanning incident detected on client
    - DDOS Attack detected on client.

*Note: The notification for Intrusion Prevention can be sent through emails only.*

6. Under **Device Control**, select the mediums through which you want to get notification for any of the following incidents:

- Attempt to access unauthorized device

*Note: The notification for Device Control event can be sent through email only.*

7. Under **Application Control**, select the mediums through which you want to get notification for any of the following incidents:
  - Attempt to access unauthorized application  
*Note: The notification for Application Control event can be sent through email only.*
8. Under **Update**, select the mediums through which you want to get the notification for the following incidents:
  - Service pack is available
  - Clients are not updated to latest virus definitions
  - Update Manager virus definition date is older  
*Note: The notification for Clients is not updated event can be sent through email only.*
9. Under **Install through Active Directory**, select the mediums through which you want to get the notification for the following incidents:
  - Synchronization with Active Directory failed
10. Under **Clients**, select the mediums through which you want to get notification for any of the following incidents:
  - Client disconnected from the network on infection
  - Client disconnected from the network on DDOS Attack
  - Client disconnected from the network on Port Scan  
*Note: The notification for all incidents can be sent through email only.*
11. Under **License related**, select the mediums through which you want to get notification for any of the following incidents:
  - License expired
  - License is about to expire
  - License limit exceeds
12. To save your setting, click **Apply**.

### **Configuring Email & SMS for Event Notification**

To configure Email & SMS Event Notification, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > Notification**.
3. In Configure Email & SMS for Event Notification, click **Configure**.  
*The Email & SMS Notification prompt appears.*
4. In the List of Email IDs, type an email address and then click **Add**.  
*You can enter multiple email addresses.*
5. In the List of Mobile Numbers, type a mobile number and then click **Add**.

6. To save the email addresses and mobile numbers, click **Apply**.

7. To save your setting, click **Apply**.

Note: For receiving email notifications, you'll need to configure SMTP settings first.



Currently notification through SMS facility is available only for the users based in India.

For some events, SMS Notification may not be applicable.

Mobile numbers listed in the National Do Not Call Registry (DND) list may or may not be able to receive notification depending on the Indian government's current telephone regulatory policies.

### **Buy Now**

This feature helps you buy Quick Heal Endpoint Security SMS bundle for sending notification.

**Number of sms left** displays how many SMS notifications can be sent. As you send the notifications, this limit is consumed. . To continue sending notification, you need to have SMS limit that you can increase by buying the SMS bundle.

You can buy the SMS bundle in any of the following ways:

- By clicking the **Buy Now** link: This link will redirect you to the portal of **Quick Heal Endpoint Security SMS bundle for notification** where you can buy SMS bundle.
- By visiting the online portal directly: You can also visit the online portal directly to buy the SMS bundle. The URL for SMS bundle is <http://www.quickheal.com/in/en/psms>.

*Note: The SMS notification bundle can be bought only if the users are based in India.*

On the shopping portal, follow the instructions about how to buy the SMS bundle.

As soon as you buy the SMS bundle, the limit in the **Number of sms left** option gets updated with due limit. If you find that the limit has not been reflected, you can update it by clicking the Update License Information button.

You can refresh the SMS bundle limit by updating the license information in the following way:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Home** tab.
2. On the Home page, click the **View License** link.
3. On the License Manager, click the **Status** button.
4. On the License Status screen, click the **Update License Information** button.

*Your license is refreshed to display the updated balance.*

## SMTP Settings

This feature helps you set the SMTP Host Details. All emails from Endpoint Security Server such as Notification mails and Report mails will be sent to the following SMTP Server for further routing:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > SMTP Settings**.
3. In the **SMTP Server** text box, type the IP Address or domain name of SMTP server.
4. In the **Port** text box, type the port number.
5. In the **User name** text box, type the user name.  
*The User name field depends on your SMTP server. It may ask you to provide either user name or email ID.*
6. In the Password text box, type the password.
7. In the **Notify from Email Address** text box, type the email address. This email address will appear as From Address in all emails sent from EPS server.
8. To apply your settings, click **Apply**.

## Add Device

This feature helps you get the details of removable devices and then add such devices to the Manage Removable Devices list. The devices added here are listed in the Device Control feature under the Settings menu (Settings > Client Settings > Device Control) where you can apply different policies to different devices to manage them better.

To add a device, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > Add Device**.
3. Plug a removable device to the system and click **Add** to fetch its details.  
*The devices details include Serial number, Manufacturer, Size, and Device name.*
4. You can also select the option **Make this device accessible only within your corporate network**.  
*Enabling this option makes the device inaccessible to all other system(s) that do not have Endpoint Security Client installed. This helps to prevent data leak as users cannot access the device on any other system outside your corporate network.*
5. Click **OK**.

Note:

- In case you are accessing web console on Windows Vista, turn off the 'Protected Mode' option in Internet Explorer.
- If you are unable to add devices through the web console, you can also use the Device Control Tool to add devices. This tool is available at the following location on the EPS Server: <Installation folder>\Admin\dcconfig.exe.

## Redirection

This feature helps you change the EPS Server for upgrading your EPS to new version. This helps in redirecting all the existing clients to new EPS Server and thereby using the new EPS server for communication. In case of software version upgrade, the previous version EPS Client will get uninstalled and new version of EPS Client will get installed.



The Redirection feature is not applicable for the clients with Mac operating systems.

However, Redirection is applicable for the client installed on Linux operating system only if the redirected server has the same EPS Server version.

To configure Redirection , follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > Redirection**.
3. In the **Server Name/IP** text box, type the sever name or IP address.
4. In the **Port** text box, type the Port number.
5. To apply your settings, click **Apply**.

## Manage Users

This feature helps you create a list of users of administrator level and report viewer level. Different types of users include:

### ***Super Administrator***

A Super Administrator user has access to all the features of Quick Heal Endpoint Security. A Super Administrator can create and modify Administrator users. Only such a user has the privilege to uninstall Quick Heal Endpoint Security.

There can only be one user with Super Administrator privileges. The default user name for Super Administrator is 'administrator'.

### **Administrator**

User with Administrator privileges has all the privileges of a Super Administrator, with two exceptions:

- Such a user cannot create another user with Administrator privileges.
- Such a user cannot uninstall Quick Heal Endpoint Security.

### **Report Viewer**

A user with the Report Viewer privileges can only view reports and status of features. This user has no other privileges. However, this type of users can change their own password.

### **Creating New Users**

To create a new user, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > Manage Users**.
3. On the Manage Users page, click **Add User**.

*An Add/Edit User dialogue appears.*

4. In the **User Name** text box, type the user name.
5. In the **New Password** text box, type the new password.
6. In the **Confirm New Password** text box, re-type the new password.
7. From the **Type** list, select the user type.

*The user type includes: Administrator and Report Viewer.*

8. To save you settings, click **Save**.

### **Modifying Existing Users**

To modify the settings of an existing user, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > Manage Users**.

*A list of all users appears.*

3. Click the **Edit** button next to the user that you want to edit.

*You can modify the setting according to the right privileges assigned to you.*

*The Add/Edit User dialogue appears.*

4. In the **New Password** text box, type the new password.
5. In the **Confirm New Password** text box, re-type the new password.
6. From the **Type** list, select the new type if you want.

7. To save your settings, click **Save**.

### ***Deleting Users***

To delete an existing user, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > Manage Users**.

*A list of all users appears.*

3. Click **Delete** next to the user that you want to delete.

*You can delete a user if you have the right privileges to do so.*

*A confirmation message appears.*

4. To delete the users, click **Yes**.

### **General**

This feature helps you configure the setting about when the running session should time out. The running session will time out if the current session is dormant for the time specified here.

To configure General, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > General**.

3. In the **Set session time out period** list, set time.

*You can select either 20 minutes, 30 minutes, or 60 minutes.*

4. To apply your setting, click **Apply**.

## **Inactive Clients**

### **Client Installation**

This feature helps you specify the path to the location where you want to get the client installed. By default a path is configured that you can change if required.

In order to change the Quick Heal client installation path, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.

2. On the Admin Settings page, click **Clients**.

*The Client Installation page appears.*

3. In the **Please specify client installation path** text box, type the installation path.

4. To apply the setting, click **Apply**.



The feature **Please specify client installation path** is not available in the clients with Mac and Linux operating systems.

## Inactive Client Settings

When you uninstall the Quick Heal client from a computer, the program automatically notifies the server. When the server receives this information, it removes the client icon in the computer tree subsequently.

However, if the client is removed using other methods, such as you reformat the computer hard drive or delete the client files manually, Quick Heal Endpoint Security will display the client as inactive. If a user unloads or disables the client for an extended period of time, the server also displays the client as inactive.

To protect the display of active clients, you can configure Quick Heal Endpoint Security to automatically remove inactive clients from the computer protection list.



The Inactive Client Settings feature is available only in the clients with Microsoft Windows, Mac, and Linux operating systems.

To automatically remove inactive clients, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, click **Clients**.  
*The Client Installation page appears.*
3. Under Inactive Client Settings, select **Enable automatic removal of inactive clients**.
4. In the **Remove a client if inactive for ...** list, select how many days after Quick Heal Endpoint Security considers a client is inactive.
5. To apply the setting, click **Apply**.



---

## Chapter 11. Reports

This menu provides the latest information of all clients and keeps comprehensive logs about virus incidents, policies, and updates. It gives the latest status of all the connected online clients and the last update report of the offline clients. Use these logs to assess virus protection policies of your organization and identify clients that are at a higher risk of infection. You can use these logs to verify if the clients have the latest updates.

### Client

This feature helps you view the reports of all online and offline clients. The reports of clients are available on the following modules: Virus Scan, AntiMalware Scan, Web Security, Tuneup, Device Control, Application Control, IDS/IPS, and Firewall.

#### Viewing Reports of Virus Scan

This feature helps you generate reports about whether any virus is found after scanning the clients through the Virus Protection, Scanner Scheduler, Memory Scan, and Email Protection modules.

To view reports of Virus Scan, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Client > Virus Scan**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group Name and a Computer Name.

*If you want to generate reports for a group, leave the computer name text box blank. If you want to generate reports for a computer name, enter the computer name in the text field. The reports will be generated for that computer name.*

5. Select the Report Type.

*The report can be displayed both in Chart and Tabular forms.*

6. To generate the report on the selected parameters, click **Generate**.

*If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as CSV or PDF.*

This report page displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when the report is generated.
<b>Computer Name</b>	Displays the name of the computer.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>File Name</b>	Displays the file names that are infected with viruses.
<b>Virus Name</b>	Displays the virus names that infect the files.
<b>Action Taken</b>	Displays the actions that were taken against viruses.
<b>View Details</b>	Displays further details for a report. To view the details, click the View Details link.

### Viewing Reports of AntiMalware Scan

This feature helps you generate reports about whether any malware is found after scanning the clients through the Schedule Scan and On Demand Scan modules (Clients > Client Action > Scan).

To view reports of Antimalware Scan, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Client > AntiMalware Scan**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group Name and a Computer Name.

*If you want to generate reports for a group, leave the computer name text box blank.  
If you want to generate reports for a computer name, enter the computer name in the text field. The reports will be generated for that computer name.*

5. Select the Report Type.

*The report can be displayed both in Chart and Tabular forms.*

6. To generate the report on the selected parameters, click **Generate**.

*If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as CSV or PDF.*

This report page displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when the report is generated.
<b>Computer Name</b>	Displays the name of the computer.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>Name of Malware</b>	Displays the malware names.
<b>Type of Malware</b>	Displays the malware types.
<b>Action Taken</b>	Displays the actions that were taken against the malware attack.

## Viewing Reports of Web Security

This feature helps you generate reports on whether any websites were blocked through the Browsing Protection, Phishing Protection, or block websites modules (Settings > Client Settings > Web Security).

To view reports of Web Security, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Client > Web Security**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a group name and a computer name.

*If you want to generate reports for a group, leave the computer name text box blank. If you want to generate reports for a computer name, enter the computer name in the text field. The reports will be generated for that computer name.*

5. Select the Report Type.

*The report can be displayed both in Chart and Tabular forms.*

6. To generate the report on the selected parameters, click **Generate**.

*If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as CSV or PDF.*

Note: In case of Business flavor of Quick Heal Endpoint Security only the Tabular format report for Web Security is available.

This report page displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when the report is generated.
<b>Computer Name</b>	Displays the name of the computer.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>Blocked Websites</b>	Displays the websites that were blocked.
<b>Category</b>	Displays the category the blocked websites belong to.

## Viewing Reports of Tuneup

This feature helps you generate reports on how many clients were tuned up and how many were not tuned up at all (Clients > Client Action > Tuneup).

To view reports of Tuneup, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Client > Tuneup**.

*The reports are displayed in chart format.*

3. To generate reports for a group, select the Group Name.
4. Select the Report Type.  
*The report can be displayed both in Chart and Tabular forms.*
5. To generate the report on the selected parameters, click **Generate**.  
*If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can print it or can also save it as CSV or PDF.*

This report page displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when Tuneup is performed.
<b>Computer Name</b>	Displays the name of the computer.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>Tuneup Status</b>	Displays whether the client was tuned up.
<b>Last Performed</b>	Displays when last Tuneup was performed.

### Viewing Reports of Device Control

This feature helps you generate reports on polices for device control such as whether removable devices have been blocked and what actions were taken against unauthorized devices (Settings > Client Settings > Device Control).

To view reports of Device Control, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Client > Device Control**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group Name and a Computer Name.  
*If you want to generate reports for a group, leave the computer name text box blank. If you want to generate reports for a computer name, enter the computer name in the text field. The reports will be generated for that computer name.*
5. Select the Report Type.  
*The report can be displayed both in Chart and Tabular forms.*
6. To generate the report on the selected parameters, click **Generate**.  
*If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as CSV or PDF.*

This report page for Device Control displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when the report is generated.
<b>Computer Name</b>	Displays the name of the computer.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>User Name</b>	Displays the user name that belongs to the domain.
<b>Device</b>	Displays the devices that have been blocked.
<b>Action Taken</b>	Displays the actions that were taken against the violation of the device control policy.

### Viewing Reports of Application Control

This feature helps you generate reports on how many applications were accessed or installed or whether they were authorized or unauthorized applications.

The reports on Application Control can be generated for On Access Scan and Application Installed separately.

#### On Access Scan

To view reports for On Access Scan, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Client > Application Control**.
3. On the General Reports page, click the **On Access Scan** tab to generate reports on the applications that were accessed.
4. Select the start and end dates for the reports.
5. Select a Group Name and a Computer Name.

*If you want to generate reports for a group, leave the computer name text box blank.  
If you want to generate reports for a computer name, enter the computer name in the text field. The reports will be generated for that computer name.*

6. Select the Report Type.

*The report can be displayed both in Chart and Tabular forms.*

7. To generate the report on the selected parameters, click **Generate**.

*If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as CSV or PDF.*

This report page displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when the report is generated.
<b>Computer Name</b>	Displays the name of the computer for which the report is generated.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>User Name</b>	Displays the user name that belongs to the domain.
<b>Blocked Application</b>	Displays the applications that were blocked.
<b>Application Version</b>	Displays the version of the applications that were blocked.
<b>Application Category</b>	Displays the category of the blocked applications.
<b>Application Path</b>	Displays the path of the blocked applications where they were installed.

***Application Installed***

To view reports for Application Installed, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Client > Application Control**.
3. On the Generate Reports page, click the **Application Installed** tab to generate reports.
4. Select a Group Name and a Computer Name.

*If you want to generate reports for a group, leave the computer name text box blank. If you want to generate reports for a computer name, enter the computer name in the text field. The reports will be generated for that computer name.*

5. To generate the report on the selected parameters, click **Generate**.

*You can take the print of the generated report or can also save the report as CSV or PDF using the respective buttons.*

This report page displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when the report is generated.
<b>Computer Name</b>	Displays the name of the computer for which the report is generated.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>Group Name</b>	Displays the group name that the selected client belongs to.
<b>Module Name</b>	Displays the module name that scanned the applications.
<b>Summary</b>	Displays the summary of the installed applications.
<b>View Details</b>	Displays further details of the installed applications. To view the details, click the View Details link. It also includes information of what authorized and unauthorized applications are present on client machine.

## Viewing Reports of IDS/IPS

This feature helps you generate reports on whether there was any Port scanning attack, DDOS (Distributed Denial of Service) attack, or any attempt of intrusion, and what actions were taken.

To view reports of IDS/IPS, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Client > IDS/IPS**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a group name and a computer name.

*If you want to generate reports for a group, leave the computer name text box blank. If you want to generate reports for a computer name, enter the computer name in the text field. The reports will be generated for that computer name.*

5. In Report For, select the attack type for which the report is to be generated.

*The report can be generated for the following modules: Intrusions Prevention, Port Scanning, and DDOS Attack.*

6. To generate the report on the selected parameters, click **Generate**.

*You can take the print of the generated report or can also save the report as CSV or PDF using the respective buttons.*

This report page on Intrusion Prevention displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when the report is generated.
<b>Computer Name</b>	Displays the name of the computer for which the report is generated.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>Vulnerability Detected</b>	Displays the vulnerability detected in a client.
<b>Action Taken</b>	Displays the actions that were taken against the attack.
<b>View Details</b>	Displays further details of the installed applications. To view the details, click the View Details link.

This report page on Port Scanning displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when the report is generated.
<b>Computer Name</b>	Displays the name of the computer for which the report is generated.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>Attacker IP</b>	Displays the IP address of the attacker.
<b>Attacker MAC Address</b>	Displays the MAC address of the attacker.
<b>Scanned Ports</b>	Displays the Ports that were scanned.
<b>Action Taken</b>	Displays the actions that were taken against the attack

This report page on DDOS displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when the report is generated.
<b>Computer Name</b>	Displays the name of the computer for which the report is generated.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>Attacker IP</b>	Displays the IP address of the attacker.
<b>Attacker MAC Address</b>	Displays the MAC address of the attacker.
<b>Action Taken</b>	Displays the actions that were taken against the attack.

## Viewing Reports of Firewall

This feature helps you generate reports on the protection policy for Firewall such as the blocked traffic for communications (Inbound or Outbound) and Firewall security level (Settings > Client Settings > Firewall).

To view reports of Firewall, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Client > Firewall**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a group name and a computer name.

*If you want to generate a report for a group, leave the computer name text box blank. If you want to generate a report for a computer name, select the group name and then type a computer name. The report will be generated for the computer name that belongs to the selected group.*

5. To generate the report on the selected parameters, click **Generate**.

*If you generate the report in chart format, you can print the report by clicking the Print option. If you generate the report in tabular format, you can also save the report as CSV or PDF.*



This report page on Firewall displays the following details of the clients:

<b>Date and Time</b>	Displays the date and time when the report is generated.
<b>Computer Name</b>	Displays the name of the computer for which the report is generated.
<b>Domain</b>	Displays the domain to which the selected client logs in.
<b>Local IP</b>	Displays the local IP address.
<b>Remote IP</b>	Displays the remote IP address.
<b>Protocol</b>	Displays the Protocol name.
<b>Direction</b>	Displays the direction of the blocked communication traffic.
<b>Firewall Level</b>	Displays the level of the Firewall security policy.
<b>View Details</b>	Displays further details of the installed applications. To view the details, click the View Details link.

## Server

This feature helps you check the event logs of all the incidents that took place on server.

To view the event logs on Server, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, click the **Server** tab.
3. On the Event Logs page, select the category for the reports.

*You can print the report or save the report as CSV or PDF using their respective buttons. You can also delete the event logs, if you prefer.*

Delete	Helps you delete the event logs.
Print	Helps you take the print of the event logs.
CSV	Helps you save the report in CSV format.
PDF	Helps you save the report in PDF format.

## Manage

This feature helps you manage the reports generated on server and clients. You can set when the reports can be removed automatically. You can also export the reports and delete them manually.

---

## Managing Settings

This feature helps you set when to remove the reports automatically in the following way:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Manage > Settings**.
3. On the Settings page, set the following:
  - In **Automatically delete reports older than...days**, set the number of days when the reports should be deleted automatically.
  - In **Automatically email reports for past... day(s) to following recipients**, set the number of past days for which the reports are required.
  - In the Email Address text box, type the email addresses.  
*If you type multiple email IDs, separate them by a comma.*
4. Under **Email Frequency**, set frequency and time when the reports should be sent.
5. Under **Select Reports to email**, set the types of reports that you want to email.
6. To save your settings, click **Save**.

## Managing Export

This feature helps you export the reports in PDF in the following way:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Manage > Export**.
3. Under Select Criteria, select what reports you want to export from the following:
  - To export all the reports, select **All Reports**.
  - In **As per below criteria**, set the criteria such as start date and end date, select a group name, and then type a computer name.
4. Under **Select Reports**, select the modules for which you want to export the reports.  
*The modules of the flavor of Quick Heal Endpoint Security that you might have are displayed.*
5. After setting all the criteria, click **Export** to export the reports in PDF.

## Managing Delete Reports

This feature helps you delete the reports manually in the following way:

1. Log on to the Quick Heal Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Manage > Delete Reports**.
3. Under **Manually delete reports**, select one of the following options:
  - **Delete reports older than ...days**: Select the number of days to remove the reports older than the days you want to.
  - **Delete all reports**: Select this option if you want to remove all the reports generated till now.
4. Under **Select Reports**, select the report types that you want to remove from the following:
  - Clients Reports
  - Server Reports
5. After setting the criteria, click **Delete** to remove the reports.

## Chapter 12. Update Manager

Update Manager is a tool integrated with Quick Heal Endpoint Security. It is used to download and manage the updates for Quick Heal Endpoint Security. It provides you the flexibility to download the updates on a single machine. All the Quick Heal Endpoint Security clients fetch the updates from this centralized location. It also provides the facility of automatically updating Quick Heal Endpoint Security for enhancements or bug fixes. Update Manager integrated with Quick Heal Endpoint Security includes all the features that are available in the Update Manager application. Any change in settings made here will reflect in the Update Manager application.

### Update Manager Status

This feature includes information of all types of updates downloaded by Update Manager. It displays the Version, Service Pack, and the Virus Database Date of the Quick Heal product accompanying the console.

Additionally, it also provides the following details:

<b>Computer Name</b>	Displays the name of the computer where Update Manager is installed.
<b>IP Address</b>	Displays the IP address of the computer where Update Manager is installed.
<b>Status</b>	Provides the information about Update Manager, whether it is online or offline.

The two buttons available under Status are:

Buttons	Description
<b>Update Now</b>	Click this button to send a Notification from Quick Heal Endpoint Security to Update Manager to start downloading the updates. This process occurs in the background and will not be visible to the user. Click <b>Back</b> to go to the Status page.
<b>Rollback</b>	Click this button to take the Update Manager back to the previous update state. This feature will work only if <b>Always take backup before downloading new update</b> option is selected in the configuration section of the Update Manager application. The steps for performing Rollback are as follows: <ol style="list-style-type: none"> <li>1. Click the Rollback button. A pop-up window opens. The Quick Heal product for the Endpoint Security is displayed.</li> <li>2. To begin the Rollback process, click Rollback.</li> </ol>

## Update Manager Settings

The following are the features available under Update Manager Settings:

Features	Description
<b>Enable Automatic Updates</b>	Select this box to enable automatic update of Quick Heal Endpoint Security. However, this feature is enabled by default. It is recommended that you do not disable this feature.
<b>Always take backup before downloading new update</b>	Select this box to enable to take the backup of the existing updates before new updates are downloaded. These backups are used in case a rollback to previous update is required. However, this feature is enabled by default.
<b>Delete report after</b>	Select this box to enable deletion of reports automatically after the time you specify. This feature is enabled by default and the default time is 10 days.

To save you settings, click the **Apply** button.

## Alternate Update Managers

In case of large network, you can deploy multiple Update Managers on different servers. This helps in load balancing and you can configure Clients in Client Settings to take the updates from these locations.

To configure Alternate Update Managers, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console.
2. On the Home page, click the **Update Manager** link available along with the product name and details.
3. On the Update Manager page, click the **Alternate Update Manager** tab.
4. In Enter Update Manager URL, type a URL and then click **Add**.

*You can edit or delete the URL whenever required.*

## Chapter 13. License Manager

This feature allows you to manage the Quick Heal Endpoint Security licenses. You can check the status of your Quick Heal Endpoint Security license, renew your license, add new licenses to your existing setup, buy additional features packs, and update license information.

### Status

This feature helps you check the current status of your license information. To check the status of your license, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console.
2. On the Home page, click the **View License** link available along with the product name and details.
3. On the License Manager page, click the **Status** tab.

The license information includes the following details:

<b>Company Name</b>	Displays the name of the company to which Quick Heal Endpoint Security is registered.
<b>Product Name</b>	Displays the product name. Example: Endpoint Security – Total.
<b>Product Key</b>	Displays the Product Key of Quick Heal Endpoint Security.
<b>Product Type</b>	Displays the product type. Example: Regular.
<b>Installation Number</b>	Displays the installation number.
<b>License Valid till</b>	Displays expiry date of the Quick Heal Endpoint Security license.
<b>Maximum number of systems under console</b>	Displays total number of systems which can be protected with Quick Heal Endpoint Security.

### ***Update License Information***

This feature is useful to synchronize your existing license information with Quick Heal Activation Server. You can update your license information whenever required.

This is helpful in updating the following license information:

- License expiry date: If you renewed the license but the expiry date is not updated or displays the old expiry date.
- Number of SMS left: If you have purchased SMS bundle for notification but the limit has not been refreshed.

Note: If you want to renew your existing license and you do not know how to renew it or are facing any problem during renewal, you can call the Quick Heal Support team and provide your Product Key.

## **License Order Form**

This feature helps you create a license order form for an additional license, renewal of your existing license, or new feature packs. This is an offline activity and helps you only in creating the license order.

After generating an order form, take out its print, contact a vendor or dealer, and submit it. You can also send an email with the license order form to the Quick Heal sales team, we will contact you for further process.

To create a license order form, follow these steps:

1. Log on to the Quick Heal Endpoint Security web console.
2. On the Home page, click the **View License** tab.
3. On the License Manager page, click the **License Order Form** tab.
4. To create a License Addition form, select one of the following:
  - [Renew my license](#): Helps you renew your current license.
  - [Add license for new endpoints](#): Helps you buy additional licenses.
  - [Buy additional feature](#): Helps you buy additional features packs.
5. Click **Place an Order**.

*An order is created.*

- Take out a print of the form, sign on it and send it to a vendor or Quick Heal Technologies (P) Ltd. to process the order.
- You can also send an email with the order form to us.

## Renew my license

If you select the **Renew my license** option, you are redirected to the online portal of Quick Heal where you can place an order for your license renewal. As you visit the portal, your license details are displayed.

On the Quick Heal online portal, do the following:

1. Under **Product Details**, verify your product license details.
2. Under **Please provide your renewal order details**, enter **Duration for which you want to renew** and **Renew the license for** the systems.
3. Click **Submit**.

*A summary of the license renewal order is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the **Back** button and make the required changes.*

4. Enter email IDs to whom you want to send the order.
5. Click **Place a Request**.

*Your license renewal request number is generated. Save this number as you will need to quote this number in all communications related to license renewal.*

6. Click **Finish**.

## Add license for new endpoints

If you select the **Add license for new endpoints** option, you are redirected to the online portal of Quick Heal where you can place an order for additional licenses for endpoints. As you visit the portal, your license details are displayed.

On the Quick Heal online portal, do the following:

1. Under **Product Details**, verify your product license details.
2. Under **Please provide your Additional license details**, enter the number of systems for which you want additional licenses.
3. Click **Submit**.

*A summary of the additional license order is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the **Back** button and make the required changes.*

4. Enter email IDs to whom you want to send the order.
5. Click **Place a Request**.

*Your license addition request number is generated. Save this number as you will need to quote this number in all communications related to additional license order.*

6. Click **Finish**.



## Buy additional feature

If you select the **Buy additional feature** option, you are redirected to the online portal of Quick Heal where you can place an order for a license for additional features. As you visit the portal, your license details are displayed.

On the Quick Heal online portal, do the following:

1. Under **Product Details**, verify your product license details.
2. Under **Please provide details of feature packs which you wish to subscribe**, select the feature packs that you want to subscribe.
3. Click **Submit**.

*A summary of the order for feature packs is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the **Back** button and make the required changes.*

4. Enter email IDs to whom you want to send the order.
5. Click **Place a Request**.

*Your license request number for new feature packs is generated. Save this number as you will need to quote this number in all communications related to new feature packs.*

6. Click **Finish**.

---

## Chapter 14. Technical Support

Quick Heal 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 Quick Heal support executives.

### **When is the best time to call?**

Quick Heal Technologies (P) Ltd. provides technical support between 9:30 AM and 6:30 PM, Monday to Saturday IST (India Standard Time).

### **Which number to call?**

Quick Heal users can call +91 - 92722 12121.

Details that will be necessary during the call are:

- Product Key that is included in the boxed version of the products. If the product is purchased online, then the Product Key can be obtained from the email confirming the order.
- Information about the computer: 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 the computer.
- Is the computer connected to a network? If yes, contact the system administrators first. If the administrators cannot solve the problem they should contact the Quick Heal technical support.
- Details: When did the problem first appear? What were you doing when the problem appeared?



Very often this information helps us to resolve your problem quickly.

### **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 input.

**Global Support Center**

Telephone Support: +91- 92722 33000.

Email: [support@quickheal.com](mailto:support@quickheal.com)

**Online Support**

Submit your query at <http://quickheal.com/submitticket.asp>.

Online chat is available at <http://quickheal.com>.

**Contact Quick Heal Technologies**

Head Office

Quick Heal Technologies (P) Ltd.

603, Mayfair Towers II,

Wakdewadi, Shivajinagar,

Pune 411 005, Maharashtra

Email: [support@quickheal.com](mailto:support@quickheal.com)

For more details, please visit: [www.quickheal.com](http://www.quickheal.com).