

# **Administrator Guide**

## **Thirtyseven4 Endpoint Security 5.2**

**TSEPS Total**  
**TSEPS Business**

Thirtyseven4, LLC  
<http://www.thirtyseven4.com>

# Copyright Information

Thirtyseven4, LLC.

## **All Rights Reserved**

All rights are reserved by Thirtyseven4, LLC.

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 transmission in any form without prior permission of Thirtyseven4, LLC, P. O. Box 1642, Medina, Ohio 44258.

Marketing, distribution or use by anyone outside of Thirtyseven4, LLC constitutes grounds for legal prosecution.

## **Trademarks**

Thirtyseven4 is a registered trademark of Thirtyseven4, LLC.

# End-User License Agreement

By using or installing any software product created by Thirtyseven4, L.L.C. an Ohio limited liability company having a principal place of business at P.O. Box 1642, Medina, Ohio 44258 (hereafter referred to as "Company") including software components, source code, object code, and the corresponding documentation (herein referred to as "Software"), you (herein referred to as "User"), are agreeing to be bound by the terms and conditions of this Agreement.

## 1. License Grant and Restrictions

In consideration for the license fee paid at time of purchase and subject to the conditions set forth in this Agreement, Company grants to User, a non-exclusive, non-sublicensable, non-assignable, non-transferable, worldwide right to use the Software.

User may only use the Software on one single computer. User may install the Software on a network, provided User has a licensed copy of the Software for each and every computer that can access the Software on the network.

User may not resell, rent, lease, distribute or transfer the Software in any way.

## 2. Fees

In consideration for use of the Software, User has agreed to pay Company the amount set forth on [www.thirtyseven4.com](http://www.thirtyseven4.com), Company's primary website, or the amount agreed to in writing between User and Company. USER EXPRESSLY ACKNOWLEDGES THAT PRIOR TO SUBMITTING ANY PAYMENT TO COMPANY OR USING THE SOFTWARE, THAT USER HAS REVIEWED AND AGREED TO BE BOUND BY THE TERMS OF THIS AGREEMENT.

## 3. Ownership

The Software and all intellectual property rights, including collateral and/or derivative rights associated therewith are the property of Company. Should any of rights relating to the forgoing become vested in User or a third party by User's use of the Software, User shall immediately transfer and/or take all steps necessary, and without compensation to Company, to insure that all right, title and interest in the same vest fully and completely in Company.

The Software and any accompanying materials are copyrighted and contain proprietary information. Unauthorized copying of the Software or accompanying materials even if modified, merged, or included with other software, or of any documentation or written materials, is expressly forbidden. However, User may make one (1) copy of the Software solely for backup purposes provided all proper legal notices are reproduced in their entirety on the backup copy. Company reserves all rights not specifically granted to User.

The Software and documentation are licensed, not sold, to User. User may not rent, lease, display or distribute copies of the Software to others except under the conditions of this Agreement.

#### **4. Termination**

This Agreement is effective until terminated. This Agreement will terminate immediately and automatically without notice from Company for failure to comply with any provision contained herein or if the funds paid for the license are refunded or are not received.

Company also may terminate this Agreement with or without cause at any time by providing notice to User of its intent to Terminate. Should Company elect to terminate this Agreement under this provision and Customer has not violated any provision of this Agreement, Company shall refund any fees paid by User to Company during the twelve months that preceded the termination.

User agrees that if User desire to terminate this Agreement, that Company shall determine in its sole and absolute discretion whether or not to refund part or all of any fee paid by User for the Software. Therefore, User expressly acknowledges that User has no right to any refund.

Upon termination, User shall destroy the Software and all copies, in part and in whole, including modified copies, if any.

#### **5. Warranties and Indemnities**

Although efforts have been made to assure that the Software is date compliant, correct, reliable, and technically accurate, the Software is licensed to User "as is" and without warranties as to performance of merchantability, fitness for a particular purpose or use, or any other warranties whether expressed or implied. User assumes all risks when using it.

EXCEPT AS OTHERWISE EXPRESSLY STATED HEREIN, THERE ARE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, AS TO THE VALUE, CONDITION, DESIGN, FUNCTIONING OF THE SOFTWARE, OR ANY USE OF THE SOFTWARE, MERCHANTABILITY, FITNESS FOR ANY PURPOSE OR USE OF THE SOFTWARE, FREEDOM FROM INFRINGEMENT OR ANY OTHER REPRESENTATION OR WARRANTY WHATSOEVER WITH RESPECT TO THE SOFTWARE. COMPANY SHALL NOT BE LIABLE TO ANY USER OF THE SOFTWARE, FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, LIABILITY, LOSS OR DAMAGE CAUSED OR ALLEGED TO HAVE BEEN CAUSED BY THE SOFTWARE, EVEN IF COMPANY WAS AWARE OF THE POTENTIAL FOR SUCH DAMAGES AND LOSS TO OCCUR.

USER SHALL DEFEND, INDEMNIFY AND HOLD HARMLESS COMPANY, ITS LICENSORS, DEALERS, INDEPENDENT CONTRACTORS, SHAREHOLDERS, DIRECTORS, EMPLOYEES, OFFICERS, AFFILIATES AND AGENTS, AND THE RESPECTIVE SHAREHOLDERS, DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES AND AGENTS OF EACH OF THE FOREGOING, FROM AND AGAINST ANY AND ALL CLAIMS, ACTIONS, JUDGMENTS, LIABILITIES, COSTS AND EXPENSES (INCLUDING LEGAL FEES) RELATING TO OR ARISING FROM THE USE OR DISTRIBUTION OF USER APPLICATIONS OR SERVICES PROVIDED BY USER (INCLUDING, BUT NOT LIMITED TO, CLAIMS RELATING TO LIABILITY FOR INFRINGEMENT OF PROPRIETARY RIGHTS, INTELLECTUAL PROPERTY RIGHTS, U.S. EXPORT AND IMPORT LAWS, DEFECTIVE PRODUCTS, OR PRODUCT LIABILITY CLAIMS).

User expressly acknowledges that any modification of the Software, whether or not permitted, is beyond the control of Company, and as such, such modification shall void any warranties, express or implied, under this Agreement.

## **6. Controlling Law and Severability**

This Agreement shall be governed by and construed in accordance with the laws of the United States and the State of Ohio, as applied to agreements entered into and to be performed entirely within Ohio between Ohio residents. The federal and state courts of the State of Ohio, County of Medina, shall have exclusive jurisdiction and venue over any dispute, proceeding or action arising out of or in connection with this Agreement or User's use of the Software. If venue is appropriate in federal court and that federal court is not located in Medina County, User and Company agree to litigate any disputes in a federal court located in Cuyahoga County, Ohio. If for any reason a court of competent jurisdiction finds any provision of this Agreement, or portion thereof, to be unenforceable, that provision of the Agreement shall be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement shall continue in full force and effect.

## **7. Non-Binding Mediation**

Company and User agree to submit the dispute to non-binding mediation before resorting to litigation. Mediation shall occur in Medina, Ohio before a single mediator jointly selected by the parties. The parties agree to each pay one-half of the mediator's fee. Company and User agree to waive any possible arbitration claims unless Company and User later agree to arbitrate this dispute following mediation, wherein such arbitration shall be binding and incur in lieu of litigation.

## **8. Limitation of Liability and Fees**

COMPANY'S TOTAL LIABILITY, INCLUDING ANY DAMAGES, SHALL NOT EXCEED THE TOTAL AMOUNT USER PAID TO COMPANY. SHOULD COMPANY BE FORCED TO MEDIATE, ARBITRATE, OR LITIGATE ANY DISPUTE AGAINST USER AND SHOULD COMPANY PREVAIL IN SUCH DISPUTE, USER SHALL REIMBURSE COMPANY FOR ALL OF ITS ATTORNEY FEES AND COSTS ASSOCIATED WITH THE ENTIRE DISPUTE, INCLUDING FEES OR COSTS INCURRED PRIOR TO ANY CLAIM BEING FILED AND ALL OF COMPANY'S COSTS, INCLUDING ATTORNEY'S FEES, ASSOCIATED WITH THE MEDIATION, ARBITRATION, OR LITIGATION.

## **9. Non-Waiver**

The failure by Company at any time to enforce any of the provisions of this Agreement or any right or remedy available hereunder or at law or in equity, or to exercise any option herein provided, shall not constitute a waiver of such provision, right, remedy or option or in any way affect the validity of this Agreement. The waiver of any default by Company shall not be deemed a continuing waiver, but shall apply solely to the instance to which such waiver is directed.

## **10. Successors; Assigns**

This Agreement shall be binding on and inure to the benefit of the parties and their respective successors and permitted assigns. Except as provided for herein, this Agreement may not be assigned by User without the prior written consent of Company.

## **11. Use of Site Image**

User grants a perpetual, world-wide, royalty-free license to Company to use and publish one or more screen shot captures of any User web sites using the Software, User's trademarks, logos or names and/or otherwise list User as a licensee of Company; provided, however, no such license shall be granted to Company if User sends an e-mail to Company stating objecting to such license within ten (10) days of receiving the Software.

## **12. Complete Agreement**


This Agreement constitutes the complete agreement between User and Company. No amendment or modification may be made to this Agreement except in writing signed by User and Company.

Please contact us with any questions or concerns regarding this Agreement.

# About This Document

This Administrator Guide covers all the information about how to install and how to use Thirtyseven4 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 Thirtyseven4 Endpoint Security</b>	<b>1</b>
How Does Thirtyseven4 Endpoint Security Work?	2
Network Deployment Scenarios	3
<i>Scenario 1</i>	3
Title	3
Network Setup Description	3
Network Representation	3
Thirtyseven4 Recommendation	4
<i>Scenario 2</i>	4
Title	4
Network Setup Description	4
Network Representation	4
Thirtyseven4 Recommendation	5
<i>Scenario 3</i>	5
Title	5
Network Setup Description	5
Network Representation	5
Thirtyseven4 Recommendation	6
<b>Chapter 2. Getting Started</b>	<b>7</b>
Prerequisites	7
System Requirements	7
Installing Thirtyseven4 Endpoint Security	10
Installing Multiple Thirtyseven4 Endpoint Security Server	13
<b>Chapter 3. Post Installation Tasks</b>	<b>15</b>
Registration	15
<i>Registering Online</i>	15
Reactivation	16
<i>Reactivating Thirtyseven4 Endpoint Security</i>	16
Renewal	16
<i>Renewing Online</i>	17
Configuring Update Manager	18
<i>How to Open Update Manager</i>	18
Uninstalling Thirtyseven4 Endpoint Security	21
<b>Chapter 4. About Thirtyseven4 Endpoint Security</b>	<b>23</b>
Home Page	23
<b>Chapter 5. Clients</b>	<b>26</b>
Client Status	26
Client Action	26
<i>Scan</i>	27



---

Scan Settings.....	28
<i>Update</i> .....	29
<i>Tuneup</i> .....	29
Tuneup Settings.....	30
<i>Application Control Scan</i> .....	31
Scan Settings.....	32
<b>Chapter 6. Client Deployment.....</b>	<b>33</b>
Through Active Directory .....	33
<i>Synchronizing with Active Directory</i> .....	34
Exclusion .....	35
Remote Install .....	36
Notify Install .....	38
Client Packager.....	39
Login Script.....	40
<i>Installing Login Script</i> .....	40
<i>Opening Login Script Setup</i> .....	40
<i>Assigning Login Script</i> .....	40
Installing EPS Clients on Mac Operating Systems .....	41
Disk Imaging .....	42
Firewall Exception Rules .....	42
Remote Uninstall.....	43
<b>Chapter 7. Manage Groups .....</b>	<b>44</b>
Adding a Group.....	44
Adding a Subgroup .....	44
Renaming a Group .....	45
Deleting a Group.....	45
Setting Policy to a Group .....	46
Changing Group of a Client .....	46
Importing from Active Directory.....	46
<b>Chapter 8. Manage Policies .....</b>	<b>48</b>
Understanding Security Policy Scenario.....	48
Creating Polices .....	50
<i>Importing and Exporting Policies</i> .....	51
<b>Chapter 9. Settings.....</b>	<b>53</b>
Client Settings.....	53
<i>Scan Settings</i> .....	53
Scanner Settings .....	54
Virus Protection Settings.....	55
DNAScan Settings .....	55
Block suspicious packed files .....	56
Automatic Rogueware Scan Settings .....	56
Disconnect Infected Clients from the network.....	56

---

Exclude Files and Folders.....	57
Exclude Extensions .....	58
<b>Email Settings.....</b>	<b>58</b>
Email Protection.....	58
Trusted Email Clients Protection.....	59
Spam Protection .....	59
<b>External Drives Settings.....</b>	<b>61</b>
External Drives Settings.....	62
Autorun Protection Settings .....	62
<b>IDS/IPS.....</b>	<b>62</b>
<b>Firewall.....</b>	<b>64</b>
<b>Web Security .....</b>	<b>66</b>
Browsing Protection Settings .....	67
Phishing Protection Settings .....	67
Web Categories .....	68
<b>Application Control.....</b>	<b>70</b>
<b>Device Control .....</b>	<b>72</b>
<b>Update Settings .....</b>	<b>74</b>
<b>Internet Settings.....</b>	<b>75</b>
<b>General Settings.....</b>	<b>76</b>
<b>Schedule Settings .....</b>	<b>77</b>
Client Scan .....	77
Application Control.....	79
Tuneup .....	80
<b>Chapter 10. Admin Settings .....</b>	<b>82</b>
Server .....	82
Password.....	82
Notification.....	82
SMTP Settings.....	85
Add Device .....	85
Redirection .....	86
Manage Users .....	86
General.....	88
Client Installation .....	88
Inactive Client Settings .....	89
<b>Chapter 11. Reports.....</b>	<b>90</b>
Clients .....	90
Viewing Reports of Virus Scan .....	90
Viewing Reports of AntiMalware Scan .....	91
Viewing Reports of Web Security .....	92
Viewing Reports of Tuneup.....	92
Viewing Reports of Device Control .....	93

---

Viewing Reports of Application Control.....	94
Viewing Reports of IDS/IPS.....	96
Viewing Reports of Firewall .....	97
Server .....	98
Manage .....	98
Managing Settings .....	99
Managing Export.....	99
Managing Delete Reports .....	100
<b>Chapter 12. Update Manager .....</b>	<b>101</b>
Update Manager Status .....	101
Update Manager Settings.....	102
Alternate Update Managers.....	102
<b>Chapter 13. License Manager .....</b>	<b>103</b>
Status.....	103
License Addition.....	104
License Renewal .....	104
License Order Form .....	105
<b>Chapter 14. Technical Support .....</b>	<b>106</b>
<i>Contact Thirtyseven4 Support Center .....</i>	<i>106</i>

# Introducing Thirtyseven4 Endpoint Security

For every organization, security of valuable data and resources is of paramount concern. Today web technology is a critical part of business processes for organizations. This puts them more at risk from emerging threats and attacks. Thirtyseven4 Endpoint Security (TSEPS) 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, hackers and so on.

TSEPS is a Web-based management solution that integrates desktops, laptops and network servers and gives access to all clients and servers in the network. TSEPS coordinates deployment of antivirus software applications, security policies, signature pattern updates and software updates on every client and server remotely. It monitors clients to check any possibilities of policy breaches and security threats within the organization, and takes appropriate action for ensuring security across the networks.

Thirtyseven4 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 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, TSEPS installation date and the date when the protection software was updated with latest virus database, security features enabled, etc.

## **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 computer or computers in a group, customize scan settings and stop scanning as per your preference. You can update the TSEPS virus database for any number of selected computers. 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 also verify security compliance by checking whether any unauthorized applications are installed anywhere within the network.

### **Client Deployment**

Helps you synchronize with Active Directory groups to deploy Endpoint Security Client and install Endpoint Security Client on a computer remotely. It allows compression of Thirtyseven4 client setup and update of files into a self-extracting file to simplify delivery through email, CD-ROM, or similar media. Helps you enable login script setup to deploy Client on remote systems when they log on to the selected domain. Enables deployment through imaging, and supports remote uninstallation of client.

### **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 various 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 Thirtyseven4 Endpoint Security Work?**

Thirtyseven4 Endpoint Security (TSEPS) 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 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.

Using TSEPS, the administrators can deploy Thirtyseven4 AntiVirus remotely on the specified computers, groups or domains, which are the part of the same domain. Whenever the server copy of Thirtyseven4 AntiVirus is updated, all computers configured to update from the server will be automatically updated without user intervention. TSEPS monitors these processes so that an administrator can view the computers that have Thirtyseven4 AntiVirus installed, the virus database date of Thirtyseven4, 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 Thirtyseven4 is uninstalled in any workstation(s), it reinstalls Thirtyseven4 remotely without user intervention. This keeps the computer and network safe from virus threats.

## Network Deployment Scenarios

Network Setup differs from one organization to another based on the size and the architecture of the network setup. Some organizations may prefer a simple network setup with one server and multiple clients, and some may opt for a network setup with subnets or DHCP servers. If an organization has a huge network setup, it might opt for a server with multiple LAN cards where a single server may cater to the needs of networks with different IP ranges.

Thirtyseven4 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. Each of the following scenarios provides recommendation for installing Thirtyseven4 Endpoint Security (TSEPS) suitable to the concerned network setup.

### Scenario 1

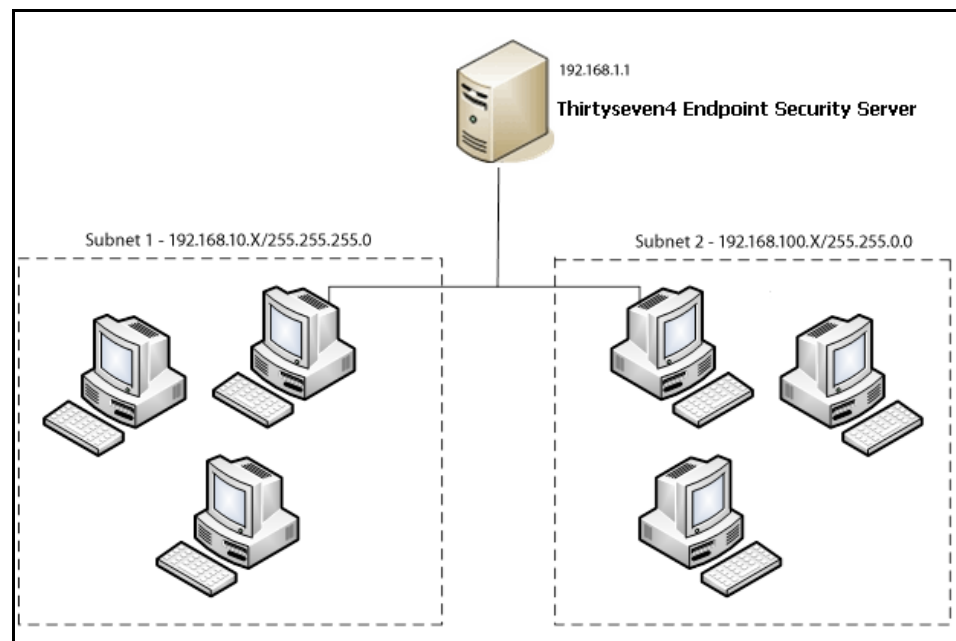
#### Title

Installing Thirtyseven4 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. Thirtyseven4 Endpoint Security will be installed on the server and Thirtyseven4 client agents will be deployed on the client systems in the subnet.

#### Network Representation



### Thirtyseven4 Recommendation

- Before installation, ensure that the server and clients are all connected by pinging server to the clients and vice-versa.
- The server system, on which Thirtyseven4 Endpoint Security will be installed, should be configured using static IP address.
- During installation of Thirtyseven4 Endpoint Security, select **IP Address** in the **Server Information Screen**.

### Scenario 2

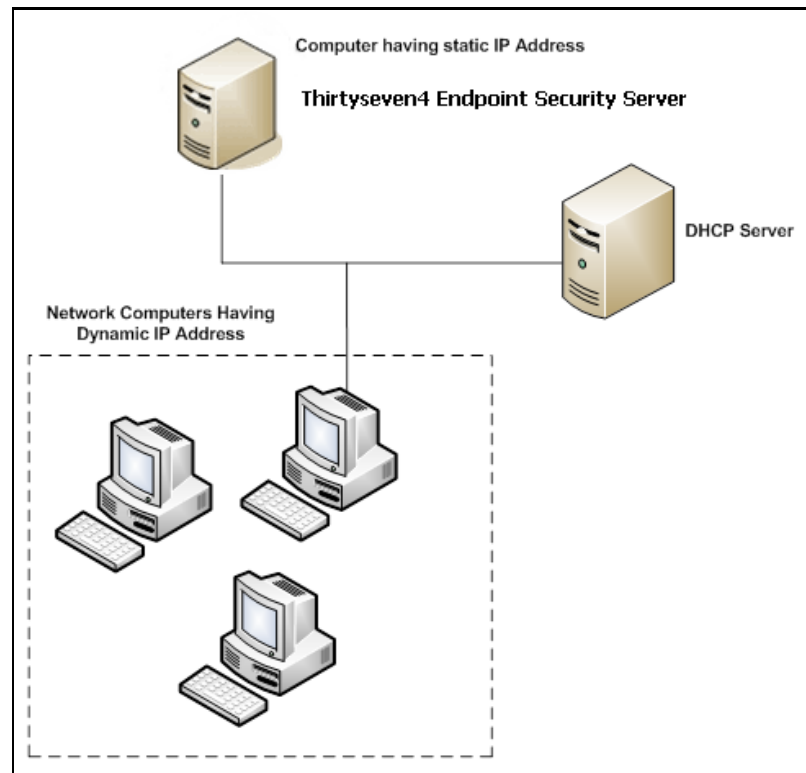
#### Title

Installing Thirtyseven4 Endpoint Security on a network with clients configured using DHCP server

#### Network Setup Description

The entire network is configured using a DHCP server. Thirtyseven4 Endpoint Security will be installed on server system and Thirtyseven4 client agents will be deployed on the client systems.

#### Network Representation



### Thirtyseven4 Recommendation

- Before installation, ensure that the server and clients are all connected by pinging server to the clients and vice-versa.
- The server system, on which Thirtyseven4 Endpoint Security will be installed, and the DHCP server system should be configured using static IP address.
- During installation of Thirtyseven4 Endpoint Security, select **IP Address** in the **Server Information Screen**.

### Scenario 3

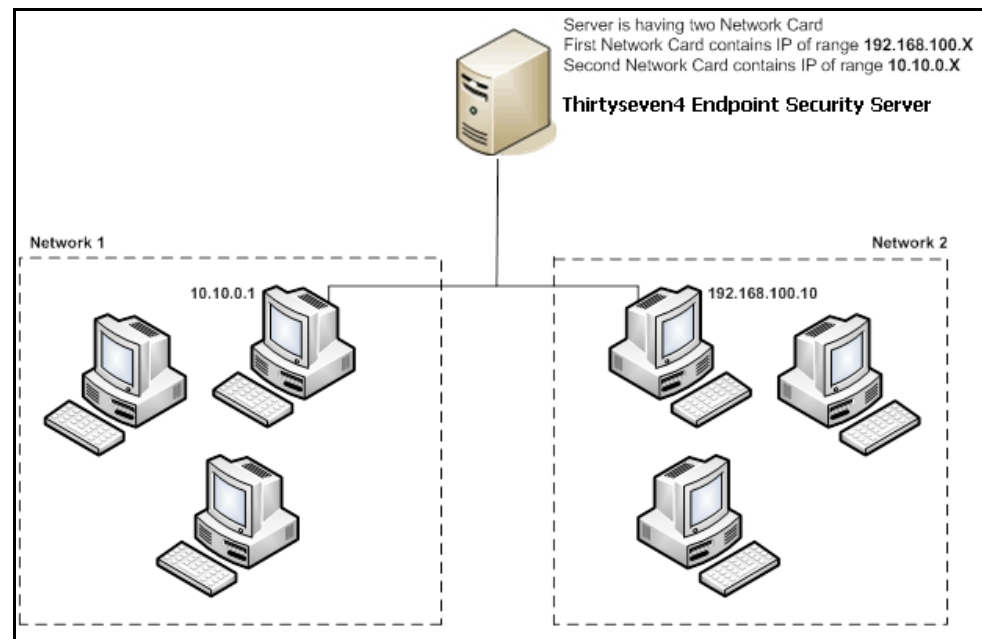
#### Title

Installing Thirtyseven4 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 Range (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). Thirtyseven4 Endpoint Security will be installed on the server with the two Network cards and Thirtyseven4 clients will be installed on all client systems of both the network.

#### Network Representation





### Thirtyseven4 Recommendation

- Before installation, ensure that the server and clients are all connected by pinging server to the clients and vice-versa. Try to ping using IP Address and System Name.
- The server system, on which Thirtyseven4 Endpoint Security will be installed, should be configured using static IP address.
- During installation of Thirtyseven4 Endpoint Security, select **Domain Name** in the **Server Information Screen**. Provide the target server domain name. You can also use the server's **Fully Qualified Domain Name (FQDN)** if the client has access to a DNS server, which can resolve the FQDN with the client's IP address.

# Getting Started

Thirtyseven4 Endpoint Security (TSEPS) 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 TSEPS on your computer:

- A machine with multiple anti-virus software applications installed may result in system malfunction. We recommend you to remove any other anti-virus software/hardware from your server and workstations before proceeding with the TSEPS installation.
- Close all open programs before proceeding with installing TSEPS.
- 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

Thirtyseven4 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
- 2700 MB of free disk space
- Monitor that supports 1024\*768 resolution at 256 colors or later

### **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 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 or later.

### ***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
- The requirement is applicable to both 32-bit and 64-bit operating systems unless specifically mentioned.

### **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
- Internet connection to receive updates

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 <http://www.thirtyseven4.com>.

## Installing Thirtyseven4 Endpoint Security

To begin installation using the Thirtyseven4 Endpoint Security DVD, follow these steps:

1. Insert the Thirtyseven4 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.

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**.

*The installation wizard appears.*

2. Click **Next**.

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

3. Click **I agree** to confirm to the license agreement and then click **Next**.

4. Click **Browse** if you wish to install Thirtyseven4 Endpoint Security on a different location. To proceed with the default installation path, click **Next**.

*The Thirtyseven4 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 Thirtyseven4 Endpoint Security on an existing IIS installation. If IIS Server is not installed /configured, you may proceed with the installation using Apache Web Server 2.0 provided in the Thirtyseven4 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**.

*The server information screen appears.*

7. 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 Thirtyseven4 Endpoint Security server address will be the following:

`http://{Thirtyseven4_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. Type an SSL port number. If you enable SSL, this port number will serve as a listening port for the server. The Thirtyseven4 Endpoint Security server address will be as follows:

`https://{Thirtyseven4_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 in.*

*The following Thirtyseven4 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.*

*Thirtyseven4 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%\Thirtyseven4\Thirtyseven4 or  
%BOOTDRIVE%\Thirtyseven4.

14. Specify the Client Agent Communication Port.

*The Thirtyseven4 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 make sure 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 Thirtyseven4 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 Thirtyseven4 Endpoint Security installation on the system.*

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

*The installation starts. Read the important information related to Thirtyseven4 Endpoint Security.*

19. Click **Next**.

20. To register Thirtyseven4 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 Thirtyseven4 Endpoint Security Server

Thirtyseven4 Endpoint Security multiple server installation is a unique feature of Thirtyseven4 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 Thirtyseven4 Endpoint Security in simple ways.

### ***Upgrading Thirtyseven4 Endpoint Security previous version to Endpoint Security latest version***

Thirtyseven4 Endpoint Security can be upgraded in the following way:

1. Install Thirtyseven4 Endpoint Security on the system where previous version of Endpoint Security is installed.
2. Thirtyseven4 Endpoint Security will detect the previous version and will show the following message:

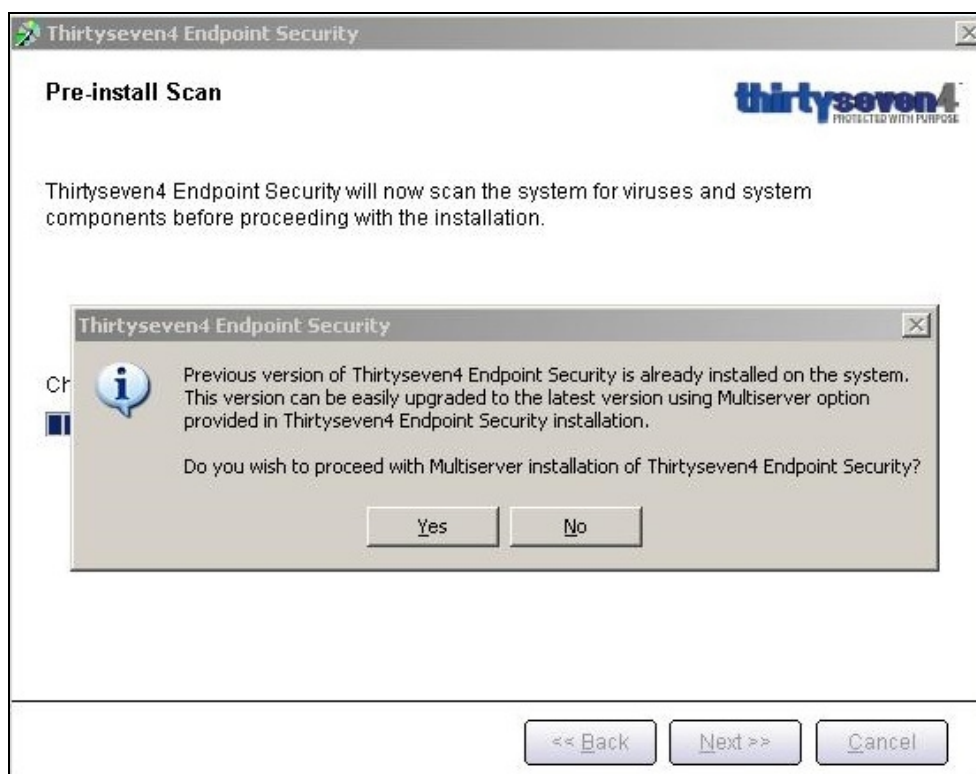


Figure 1: Pre-install Scan

3. To proceed with multiserver installation, click **Yes**.

*Upon completion of installation of the later version of Thirtyseven4 Endpoint Security, open the previous version Thirtyseven4 Endpoint Security and follow these steps:*



- i. Select **Administrator Settings > Admin Server**.
- ii. In Server Name/IP text box, type the Server Name or IP Address of the latest version of Thirtyseven4 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 to all Thirtyseven4 clients about the latest version Thirtyseven4 Endpoint Security and all Thirtyseven4 clients will be redirected to the latest version Thirtyseven4 Endpoint Security.*

4. The latest version of Thirtyseven4 Endpoint Security will check for any previous version clients in the network. Upon detection, Thirtyseven4 Endpoint Security will automatically uninstall the previous version clients and install the latest version clients.
5. Once all the clients are upgraded, you can uninstall previous version of Thirtyseven4 Endpoint Security from the system. Before uninstallation, note down the Product Key and activation number of your Thirtyseven4 Endpoint Security that will be required for re-activation of latest version of Thirtyseven4 Endpoint Security.
6. After uninstallation of previous version of Thirtyseven4 Endpoint Security, re-activate latest version of Thirtyseven4 Endpoint Security with your existing Product Key and Activation Number.



- You can upgrade all previous version clients to latest version within 30 days period only.
- If you have configured previous version of Thirtyseven4 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 Thirtyseven4 Endpoint Security site with SSL support on the operating systems mentioned in the preceding section. In this case, you can install latest version of Thirtyseven4 Endpoint Security with Apache Web Server.
- If you have installed a previous version of Thirtyseven4 Endpoint Security, do not uninstall Apache Server during uninstallation of the previous version of Thirtyseven4 Endpoint Security.

# Post Installation Tasks

Thirtyseven4 Endpoint Security must be registered immediately after installation to activate the copy, otherwise without activation client deployment will not start.

## Registration

Thirtyseven4 Endpoint Security is simple to register. You can register the product in any of the following ways:

### Registering Online

If your system is connected to the Internet, you can register Thirtyseven4 Endpoint Security online in the following way:

1. Go to **Start > Programs > Thirtyseven4 EPS Console 5.2 > Activate Thirtyseven4 EPS Console**.

*The Registration Wizard appears.*

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.*

*On successful completion of activation, 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.
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 Thirtyseven4 Endpoint Security**

Re-activation is a facility that ensures that you use the product for the full period until 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 Thirtyseven4 Endpoint Security on another computer. In such cases, you need to re-install and re-activate Thirtyseven4 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, your information 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.

## **Renewal**

You can renew your license any time after activation and within four (4) months after expiry. However, you are recommended to renew your product before your license expires so that your system is protected without any interruption. You can get a renewal key from the Thirtyseven4 website, or from the nearest distributor or reseller.

You can renew Thirtyseven4 Endpoint Security in any of the following ways.

## Renewing Online

If your system is connected to the Internet, you can renew Thirtyseven4 Endpoint Security online in the following way:

1. Go to **Start > Programs > Thirtyseven4 EPS Console 5.2 > Activate Thirtyseven4 EPS Console**.

*The Registration Wizard appears.*

2. On the registration wizard, type the Product Key and then click **Next**.

*If your current license has expired, the renewal screen displays a message about it. You can renew your license by purchasing a renewal code.*

3. In the Renewal Code text box, type the renewal code and then click **Next**.

4. On the Registration Information screen, type Purchased from and then click **Next**.

*A summary of the license information that you entered appears. Check it carefully. If you want to change the information, click **Back** to go to the previous screen and make the required changes. To confirm, click **Next**.*

*Your license is renewed successfully and the License validity information is displayed.*

5. 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 may also set authentication rule if you use Firewall or proxy sever. To set 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.*

## Configuring Update Manager

Update Manager is a tool that is used to download and manage the updates for Thirtyseven4 Endpoint Security. It provides you the flexibility to download all product updates on a single machine. It also provides the facility of automatically updating Thirtyseven4 Endpoint Security for enhancements or bug fixes. All Thirtyseven4 Endpoint Security Clients will fetch the updates from this centralized location.

### How to Open Update Manager

To open Update Manager, select **Start > Programs > Thirtyseven4 EPS Console 5.2 > 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 Thirtyseven4 product.

#### **Configuration**

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

1. Click **Start > Programs > Thirtyseven4 EPS Console 5.2 > Update Manager**.
2. Click **Configuration**.
3. Type the Super Administrator, Password and then click **OK**.

The right panel includes the following configurations:

Enable Automatic Updates	Checking this box enables automatic update of Thirtyseven4 Endpoint Security. By default, this feature is enabled. It is recommended that you do not disable this feature.
--------------------------	--

## Select the updating mode

Download from Internet Center	Selecting this option will enable downloading of the updates from the default Internet Center. By default, this feature is selected.
Download from specified URL	<p>Selecting this option will help you specify the URL for downloading the updates. In this case, the URL will be the path 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.</p> <ul style="list-style-type: none"> <li>• In Server, type the URL.</li> <li>• In Port, type the port number.</li> </ul> <p>Note: msg32.htm file should be present at the update location where the updates are downloaded in the system with Internet connection.</p> <p>To create msg32.htm file, rename a text file as msg32.htm file.</p>
Pick from specified path	<p>To take the updates from a specified folder of local system, select <b>Pick from specified path</b>. 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.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• Select the <b>Pick from specified path</b> option.</li> <li>• Enter the path to the folder where the updates have been copied in the local system.</li> </ul>

## Select the updates you want to download

Check the Thirtyseven4 product specific to your Endpoint Security, for which you need to download the updates.

Download Endpoint Security Service Pack	Checking this box enables downloading the Thirtyseven4 Endpoint Security Service Pack. By default, this feature is enabled.
---	---

## Download updates to

This text box specifies the location where the updates will be downloaded. All Thirtyseven4 Clients will take the updates from this centralized location.

Always take backup before downloading new update	Checking this box enables taking 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	Checking this box enables deletion of 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.

## Prevent unauthorized access to settings

Enable Password Protection	<p>Checking this box enables password protection. This feature also allows you to change password of Update Manager. Enabling password protection prompts you to enter the password the first time you access either Configuration or Connection Settings feature of Endpoint Security. To change the password, follow these steps:</p> <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>
----------------------------	--

To save your changes, click **Apply**.

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	Click this button to download the updates of Thirtyseven4 Endpoint Security.
Rollback	<p>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 option</b> is selected in the Configuration section of Update Manager. The steps for performing Rollback are as follows:</p> <ol style="list-style-type: none"> <li>1. Click the <b>Rollback</b> button. The Thirtyseven4 product for the Endpoint Security is displayed.</li> <li>2. Click Rollback.</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. Click **Start > Programs > Thirtyseven4 EPS Console 5.2 > 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 login 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 contains a log of updates or rollback activity. It provides details such as the Date, Time, and Status of the updates or rollback activity. To access Reports, follow these steps:

1. Click **Start > Programs > Thirtyseven4 EPS Console 5.2 > 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 Thirtyseven4 Endpoint Security**

Uninstalling Thirtyseven4 Endpoint Security may expose your systems and valuable data to virus threats. However, if you need to uninstall Thirtyseven4 Endpoint Security, follow these steps:



1. Go to **Start > Programs > Thirtyseven4 EPS Console 5.2 > Uninstall EPS Console**.

*Thirtyseven4 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 Thirtyseven4 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 Thirtyseven4 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.

# About Thirtyseven4 Endpoint Security

Web Console is also installed during the installation of Thirtyseven4 Endpoint Security. 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://{Thirtyseven4_Endpoint_Security_Server_name}:{port number}/qhscan502.`
- If using SSL, type:  
`https://{Thirtyseven4_Endpoint_Security_Server_name}:{port number}/qhscan502.`

The browser displays the Thirtyseven4 Endpoint Security login page.

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

## Home Page

Upon logging in to the Thirtyseven4 Endpoint Security console, the Home page appears from where you can access to all the features and work. The Home page displays a summary about various activities that are described as follows:

**Thirtyseven4 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 had detected viral infection in last 24 hours.
Elevated	Indicates that 24% of the clients had detected viral infection in last 24 hours.
High	Indicates that 36% of the clients had detected viral infection in last 24 hours.
Critical	Indicates that more than 36% of the clients had detected viral infection in last 24 hours.

**Important:** Thorough scanning of the entire network is recommended if Threat Level on the threat meter is 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 displays about how secure your system is. The graphical representation is displayed in four grids that have the following meaning:

Symbol	Level	Description
Green	Normal	Indicates system is not infected and is secure.
Yellow	Elevated	Indicates system is infected but at low level.
Orange	High	Indicates system is infected at high level. Immediate action is required.
Red	Critical	Indicates system is infected and is at critical level. Immediate action is required.

**View for:** Helps you display the network health in graphical representation of the time period that you prefer. You can view the graph of the following time period:

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 websites 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 the features that help you manage and control all the clients deployed in the network. You can verify the current status of the clients, carry out various activities such as scanning client computers, updating the software application, improving system performance, installing and uninstalling Thirtyseven4 Endpoint Security Client remotely, managing client groups, creating and applying scanning policies and so on.

## Client Status

With Client Status, you can view the current status of all the clients in the network. The status includes information such as the computer name, the group it belongs to, domain it belongs to, IP address, Mac address, protection status, installation status, product version, virus database date, last scan date, and protection policies among others.

To view Client Status, follow these steps:

1. Log in to Thirtyseven4 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 export the status or take a printout of it as you prefer.*

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

With Client Action, you can scan computers remotely, update virus definitions, improve performance of the computers, verify 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 Thirtyseven4 Endpoint Security clients on different operating systems:

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

## Scan

With Scan, you can scan any computer in your network remotely. This helps you avoid the task of visiting the target computer personally. You can initiate a manual scan with pre-configured policies for convenience.

To initiate scanning, follow these steps:

1. Log in to Thirtyseven4 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 computers which are not online or are disconnected from the network.
Show computers within subgroup	Helps display computers that are in a subgroup.
Scan Settings	Helps you customize scan settings.
Notify Start Scan	Helps you notify clients to start scanning.
Notify Stop Scan	Helps you notify clients to stop scanning.
Stop Notification	Helps you stop notification.

## Scan Settings

With Scan Settings, you can customize the scan settings for a client machine.

To customize scanning, follow these steps:

1. Login to Thirtyseven4 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 scanning 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 applicable only for the clients with Windows operating systems

## Update

With Update, you can remotely update client applications at any computer in the network. Thirtyseven4 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 in to Thirtyseven4 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 Thirtyseven4	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 Thirtyseven4.
Stop Notification	Helps you stop notification.

## Tuneup

With Tuneup, you can improve the performance of the computers by cleaning unwanted and junk files, invalid and obsolete registry entries, and by defragmentation. While performing various tasks, computers write junk on the drives, temporary files are created when you visit websites, these unnecessarily occupy empty spaces and slow down machines. Tuning up your machines cleans up a lot of unwanted junk thus making them lighter and improving their performance.



- The Tuneup feature is applicable only for 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 in to Thirtyseven4 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 computers which are not online or are disconnected from the network.
Show computers within subgroup	Helps display those computers that are in a subgroup.
Tuneup Settings	Helps you customize Tuneup settings.
Notify Start Tuneup	Helps you notify clients to start Tuneup.
Notify Stop Tuneup	Helps you notify clients to stop Tuneup.
Stop Notification	Helps you stop notification.

## Tuneup Settings

With Tuneup Settings, you can customize what to cleanup such as disks, registry entries, or if you want to defragment at next boot.

To customize Tuneup settings, follow these steps:

1. Log in to Thirtyseven4 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 un-install, 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

With Application Control Scan, you can check whether security compliance laid out by your organization is being followed by each endpoint. It allows you to verify whether endpoints have any unauthorized applications other than the authorized software applications running on them.



The Application Control Scan feature is applicable only for the clients with Windows operating systems.

To scan computers for compliance control, follow these steps:

1. Log in to Thirtyseven4 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 computers which are not online or are disconnected from the network.
Show computers within subgroup	Helps display computers that are in a subgroup.
Scan Settings	Helps you customize the scan settings for application control.
Notify Start Scan	Helps you notify clients to start scanning.
Notify Stop Scan	Helps you notify clients to stop scanning.
Stop Notification	Helps you stop notification.

### Scan Settings

With Scan Settings, you can customize your scan preference. To customize Scan Settings, follow these steps:

1. Log in to Thirtyseven4 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**.

## Chapter 6.

# Client Deployment

Client Deployment helps you to synchronize with Active Directory groups to deploy Thirtyseven4 Endpoint Security Client and install Endpoint Security Client on a computer remotely. It also compresses Thirtyseven4 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 Thirtyseven4 Endpoint Security Client on remote systems when they log on to the selected domain or deploy Thirtyseven4 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 Thirtyseven4 Endpoint Security clients on different operating systems:

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

## Through Active Directory

With Through Active Directory, you can sync with Active Directory groups. Once you sync the group, the clients will get installed on all computers which come under your domain network. A periodic check is carried out to find out whether 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 applicable only for 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 which are shown in Red Color are already synched with Active Directory.
- The user should have permissions of “Domain Admins” to synchronize with Active Directory.
- Synchronization time interval is GLOBAL.

## Synchronizing with Active Directory

To sync Active Directory groups, follow these steps:

1. Log in to Thirtyseven4 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 username 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

With Edit Synchronization, you can edit the time interval to carry out the check to find if a new computer is added to the network. You may need to change the frequency depending on how many and how often new computers are added.

To edit the time interval, follow these steps:

1. Log in to Thirtyseven4 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 synched 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 Remove Synchronization, you can remove the synchronization of a group.

To remove a synchronization setting, follow these steps:

1. Log in to Thirtyseven4 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 Exclusion, you can exclude certain workstations from installation of Endpoint Security Console client when Active directory is synchronized. EPS Console client will not get installed on excluded workstation. You can exclude workstations by Host Name, IP Address or IP Range.

To exclude a workstation, follow these steps:

1. Log in to Thirtyseven4 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, then 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, then 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, then 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

With Remote Install, you can deploy the Thirtyseven4 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 Thirtyseven4 client on multiple computers at a time. Before proceeding with Remote Install, you are recommended to 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 Thirtyseven4 is not supported on Windows XP Home Edition. To install the Thirtyseven4 client on Windows XP Home Edition, other methods of installation can be used, like Notify Install, Login Script, and Client Packager provided in Thirtyseven4 Endpoint Security.

- Remote Install is not supported with the users having blank passwords on Windows XP and later operating systems.
- To install Thirtyseven4 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 in to Thirtyseven4 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 of the following way:

- 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 facility.

*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, for which you need to have administrator rights of that computer.*

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

*Repeat this step 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 Thirtyseven4 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 the 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 Thirtyseven4 client agent, the installation status appears in the Result field of the selected computers list.*



The Remote Install feature is applicable only for the clients with Windows operating systems.

## Notify Install

With Notify Install, you can send email notification to the computers on your network that notifies them to install the Thirtyseven4 Endpoint Security client. You can type your message and save it for future notifications. However, you can edit the message anytime you prefer.

To notify clients to install the Thirtyseven4 client, follow these steps:

1. Log in to Thirtyseven4 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.*

The users have to click the link provided in the email. The link will open the Thirtyseven4 client installation web page. The users need to install ActiveX and click **Install** to proceed with the Thirtyseven4 client installation. After the Thirtyseven4 client installation is finished, the Thirtyseven4 AntiVirus installation will be initiated by the Thirtyseven4 client.

## Client Packager

Client Packager can compress the Thirtyseven4 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 within the Client Packager tool.

In Thirtyseven4 Endpoint Security 5.2, Client packager can be created with or without the Thirtyseven4 installer. The Client agent installer including the Thirtyseven4 installer is helpful where network bandwidth has limitations to download the Thirtyseven4 installer from the Endpoint Security server for the deployment. In such a case, create the Client agent installer including the Thirtyseven4 installer and burn into a CD/DVD or copy it into a USB removable disk for the deployment on endpoints.

When users receive the package, they just have to double-click the setup program. The Thirtyseven4 clients installed through Client Packager communicates to the Thirtyseven4 Endpoint Security server. This tool is especially useful when deploying the client setup on remote offices with low-bandwidth.

To create a Thirtyseven4 Client package, follow these steps:

1. Go to **Start > Programs > Thirtyseven4 EPS Console 5.2 > Client Packager**.
2. Select the Client Packager with or without the Thirtyseven4 installer.
3. Select the setup type such as 32-bit or 64-bit.
4. Specify the folder path where you want to save Thirtyseven4 Client Packager.
5. Click **Create**.



- The Client Packager feature is applicable only for 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 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**

With Login Script, you can assign a login script to the users so as they can deploy Thirtyseven4 Client on remote systems when they log in to the selected domain. Using Login Script, you can assign a script called QHEPS.BAT to the selected users in the domain. This script will install the Thirtyseven4 Endpoint Protection on the system when the user logs in to the concerned domain.



The Login Script feature is applicable only for the clients with Windows operating systems.

### **Opening Login Script Setup**

To open the Login Script Setup, follow these steps:

1. Click **Start > Programs > Thirtyseven4 EPS Console 5.2**.
2. Click **Login Script Setup**.
3. Type the **Super Administrator Password** of Thirtyseven4 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 Thirtyseven4 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 Thirtyseven4 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 EPS Clients on Mac Operating Systems

Before you install Thirtyseven4 Endpoint Security, you get a Notify Install message from administrator which includes a link to the web page for the installer file.

To install Thirtyseven4 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 Thirtyseven4 Endpoint Security installation.

*Thirtyseven4 Endpoint Security is installed successfully.*

## 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 applicable only for the clients with Windows operating systems.

## Firewall Exception Rules

Operating systems such as Windows have their own Firewall bundled with them. Sometimes users may prefer to retain the firewall bundled with their operating system. In such cases Thirtyseven4 Endpoint Security creates exception rules for firewalls bundled with the operating system. These exception rules are created during installation of Thirtyseven4 Endpoint Security. For the system on which Thirtyseven4 Endpoint Security is installed, the exceptions will be automatically created during installation and for the Thirtyseven4 client the exception will automatically be created during deployment of Thirtyseven4 clients.

The system with Thirtyseven4 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 Thirtyseven4 client will require one exception rule to be created. The following is the exception rule for clients:

- Client Agent 5.2

## Remote Uninstall

With Remote Uninstall, you can remove the Thirtyseven4 client along with AntiVirus program from computers on your network remotely.

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

1. Log in to Thirtyseven4 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 Thirtyseven4 client. To uninstall Thirtyseven4 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. Click **Start Uninstall Notification**.

*The uninstallation starts.*

### Stop Uninstallation Notifications

If you want to stop sending notifications to the clients that have not yet started the client uninstallation program, follow these steps:

1. Select the clients that you no longer want to remove.
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 computers which are not online or are disconnected from the network.
Show computers within subgroup	Helps display computers that are in a subgroup.

# Manage Groups

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

## Adding a Group

To add a new group, follow these steps:

1. Log in to Thirtyseven4 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 display 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 in to Thirtyseven4 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.*

Note: A subgroup is also a group except that it is under a group. Hence all the processes of managing groups or subgroups are similar. Whatever we describe about a group also applies to a subgroup.

### **Renaming a Group**

To rename a group, follow these steps:

1. Log in to Thirtyseven4 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 in to Thirtyseven4 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

A policy includes different client settings for different groups in your organization.

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

1. Log in to Thirtyseven4 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. Hover over 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

You can change the group of a client. This is helpful if you think a client should be in a certain group or you want to change the group because of policy change at your organization. Moreover, if you change the group, the protection policy of the new group will apply.

To change group of a client, follow these steps:

1. Log in to Thirtyseven4 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

With Import from Active Directory, you can import Active Directory Structure in console. This is helpful when you need to have group structure in the console that is already available in the Active Directory. You need not create the groups, you can simply import it from the Active Directory and use it.

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 in to Thirtyseven4 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 username in the format "domain name\user name" and then enter your password. Click **Next**.  
*The Select Active Directory Container screen appears.*
6. 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 then only the selected container will get imported.
8. Click the **Finish** button.

# Manage Policies

Each organization would like to enforce a policy that regulates the users about how they visit only certain websites, how to scan their systems, what the email communication policy should be for them, whether they should be allowed to use applications and work with external USB-based devices other than the organization permits, and so on. Thirtyseven4 Endpoint Security allows the administrators to create policies that helps centrally control and manage the users that belong to a group.

The Manage Policies feature of Thirtyseven4 Endpoint Security gives you the flexibility and control over creating new policies, modifying or removing an existing policy. Different protection policies can be created for different groups for better control. Each policy 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 policy.

It is recommended that you should have groups created before you create a policy setting. A group is a department in an organization and a subgroup is also a group except that it is under a group. To know about how to create a group, refer to [Adding a Group](#) in Chapter 7 “Manage Groups”, p - 44.

## Understanding Security Policy Scenario

Suppose there are two departments or groups in your organization such as Marketing and Accounts. This might require you to have different policies for each. The following may be the example of how you can create different policies for different departments. However, you may create a completely different policy from the example given herein depending on your requirement.

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
Email Settings	Email Protection	Enabled	Enabled
	Trusted Email Clients Protection	Enabled	Enabled
	Spam Protection Level	Soft	Strict
External Drives Settings	Scan External Drives	Enabled	Enabled
	Autorun Protection	Enabled	Enabled
IDS/IPS	IDS/IPS	Enabled	Enabled
	Disconnect system from the network (only in case of DDOS and Port Scanning attack)	Not Enabled	Enabled
Firewall	Firewall	Enabled	Enabled
	Level	Low	High
Web Security	Browsing Protection	Enabled	Enabled
	Phishing Protection	Enabled	Enabled
Web Categories	Business	Allowed	Denied
	Social Networking	Denied	Denied
Application Control	CD/DVD Applications	Authorized	Unauthorized
	Games	Unauthorized	Unauthorized
Device Control	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 Polices

When you apply a policy to a group or a subgroup, the inherent settings of the policy also apply. While creating policies, you should ideally ensure that you configure different policy settings from the client settings and schedule settings so different groups have different policies. However, this depends on the requirement of your organization.

Note: A subgroup is also a group except that it is under a group. Hence all the processes of applying policies are similar. Whatever we describe about a group also applies to a subgroup.

### ***Creating a new policy***

To create a new policy, follow these steps:

1. Log in to Thirtyseven4 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 in to Thirtyseven4 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 may 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 in to Thirtyseven4 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**

When you have multiple installations of Thirtyseven4 Endpoint Security on physically separated networks or in case you are planning to re-install Thirtyseven4 Endpoint Security for some reason you can have the policy configurations saved on an external file. This provides simple and easy way to configure identical settings across different installations or even during re-installation process. You can select the policy settings for exporting or importing.

### ***Exporting a policy***

To export the policy settings, follow these steps:

1. Log in to Thirtyseven4 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 exported settings file.
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 in to Thirtyseven4 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 prompt appears that allows you to select which policies you want to import.*
4. Select the policies that you want to import.
5. Click **Import**.

# Settings

With Settings, the administrators can 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 may 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 (Thirtyseven4 Endpoint Security > Clients > Manage Policies) from where you can customize its settings.

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

## Client Settings

### Scan Settings

With Scan Settings, you can define a policy about how to initiate the scan of the client systems in your organization. The policy could be refined to enable Virus Protection or DNA scanning or it about defining policies on blocking any suspicious packed files, and other settings.

The following table shows a comparison of the features in Scan Settings that are applicable for different Thirtyseven4 Endpoint Security clients on different operating systems:

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

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

1. Log in to Thirtyseven4 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 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 may 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 may 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 may 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, 53.

## Virus Protection Settings

With Virus Protection Settings, you can continuously keep monitoring the client systems for viruses that may try to infiltrate from various sources such as email attachments, Internet downloads, file transfer, file execution and so on.

It is recommended that you always keep Virus Protection enabled to keep the client systems clean and protected from any potential threats.

The following table shows a comparison of the features in Virus Protection Settings that are applicable for different flavors of Thirtyseven4 Endpoint Security clients:

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

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 may 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 against new and unknown malwares whose signatures are not present. DNAScan is an indigenous technology of Thirtyseven4 to detect and eliminate new and unknown 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 applicable only for the clients with Windows operating systems.

### Block suspicious packed files

The Block suspicious packed files feature helps you identify and block suspicious packed files from accessing. Suspicious packed files are the malicious programs that are compressed or packed using a variety of methods combined with file encryption. Such packers when unpacked can cause serious harm to computer systems.

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



The Block suspicious packed files feature is applicable only for the clients with Windows operating systems.

### Automatic Rogueware Scan Settings

The Automatic Rogueware Scan feature automatically scans and removes rogueware and fake anti-virus software of critical level. If this feature is enabled, all the files are scanned for whether there is any rogueware present in a file.



The Automatic Rogueware Scan feature is applicable only for 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 applicable only for the clients with Windows operating systems.

## Exclude Files and Folders

With Exclude Files and Folders, you can decide which files and folders should not be included during scanning for Known Viruses, DNAScan, and Suspicious Packed files. This is helpful if you trust certain files and folders so you do not include them in scanning.

The following table shows a comparison of the features in Exclude Files and Folders that are applicable for different Thirtyseven4 Endpoint Security clients on different operating systems:

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

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

1. Log in to Thirtyseven4 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 appear as selected.

If you select DNAScan, Suspicious Packed File Scan will also be enforced and both the options appear as selected.

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

## Exclude Extensions

Helps you exclude the files by their extensions from scanning by real-time virus protection. 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.*

## Email Settings

With Email Settings, you can 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 Thirtyseven4 Endpoint Security clients on different operating systems:

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

To configure Email Settings, follow these steps:

1. Log in to Thirtyseven4 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 Email Protection, you can apply the protection rules to all incoming emails. The protection rules include blocking the infected attachment in the emails that may be suspicious of malware, spams, and viruses.

To apply Email Protection to the users in a group, select Enable Email Protection. If Email Protection is enabled, all the emails that are received at the clients will be scanned before they are sent to Inbox.

### Trusted Email Clients Protection

Email is the most widely used medium of communication for all purposes now-a-days, so new viruses use email as a medium to spread. Virus authors always look for new methods to automatically execute their viral codes using some vulnerability 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 applicable only for the clients with Windows operating systems.

### Spam Protection

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

The following table shows a comparison of the features in Spam Protection that are applicable for different Thirtyseven4 Endpoint Security clients on different operating systems:

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

## Configuring Spam Protection

To configure Spam Protection, follow these steps:

1. Log in to Thirtyseven4 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:
  - **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 might block 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, 59.

### Setting spam protection rule for White List

White List is the list of email addresses from which all emails are allowed to skip the spam protection filtering rule irrespective of their content. Emails from the addresses listed here don't go through the SPAM filter. It is suggested that you configure only those email addresses that you trust completely.

To add email addresses in the White List, 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 Black List

Black List is the list of email addresses from which all emails are filtered irrespective of their content. All emails from the addresses listed here are tagged as "[SPAM] -". This feature should be especially evoked in case some server has an Open Relay which is being misused by Mass Mailers and viruses.

To add email addresses in the Black List, 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

With External Drives Settings, you can set protection rules for external devices such as CDs, DVDs, USB-based drives and so on. Whenever your system comes in contact with any external drives, your system is at risk from viruses and malwares may infiltrate through them.

The following table shows a comparison of the features in External Drives Settings that are applicable for different Thirtyseven4 Endpoint Security clients on different operating systems:

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



To configure External Drives Settings, follow these steps:

1. Log in to Thirtyseven4 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 and Autorun Protection 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.

### **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 applicable only for 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 in to Thirtyseven4 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 alert 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.

With Firewall, you can create different policies for various groups/departments such as you can enable firewall protection, apply firewall security level with an exception rule and other settings according to the requirement. 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 applicable only for the clients with Microsoft Windows.

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

1. Log in to Thirtyseven4 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	Blocks all Inbound and allows all 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. 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.  However for the exception rule with Medium security, it is advisable that you allow to receive inbound data and block outbound data to take more advantage of the security level policy.
Low	Allows all Inbound and Outbound traffic.  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.

### 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

With Web Security, you can create a security policy for a department or group where you enable Browsing Protection and Phishing Protection so the malicious or phishing sites are blocked. 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 Thirtyseven4 Endpoint Security clients on different operating systems:

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

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

1. Log in to Thirtyseven4 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

Browsing Protection ensures that malicious websites are blocked while the users in a group browse the Internet so that the users are prevented from coming in contact with malware and they are secure. When the users visit malicious websites, some files are also installed on the systems that may spread malware, slow down the system, or corrupt some files. Such attacks may harm the system, sometimes beyond repair.

The administrators can enable Browsing Protection that blocks the websites with malicious content before the users can access them. As soon as a site is visited it is scanned for whether it is a malicious website, and if so it is blocked to avoid any malicious attacks.

### Phishing Protection Settings

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. It usually appears to have come from seemingly well-known organizations and sites such as banks, companies and services with which you do not even have an account asking you to visit their site and requests you to provide your personal information such as credit card number, social security number, account number or password.

The administrators can enable Phishing Protection that prevents the users from accessing phishing and fraudulent websites. As soon as a site is visited it is scanned for whether it is a phishing site and if so it is blocked to avoid any phishing attempts.

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

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

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 Thirtyseven4 lab if it gets detected either as malicious or phishing.*

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 setting, 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 some concerns that an organization might face:

- The systems might get infected.
- Users may browse unwanted websites.
- A virus infiltrates and spreads to other systems.
- The employees idle away time.

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

The Web Categories feature of Thirtyseven4 Endpoint Security 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.

To configure Web Categories, follow these steps:

1. Log in to Thirtyseven4 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**.

*If you allow or deny a category, access to all the sites under a category will be allowed or denied.*

### **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 which are a priority to you or you trust such websites.

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 restricted category.
Delete	Helps you delete a URL from the Excluded URL list.

### **Block specified websites**

This feature is helpful when you are interested in restricting the users to access certain websites or when a website does not fall in a correct category, or you have a shorter list of the websites so you would prefer to restrict the websites than restrict 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` and select 'Also block subdomains', all its subdomains such as `mail.google.com` will also be blocked.*

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



The Also Block Subdomains feature is not applicable for the clients with Mac operating systems.



## Application Control

While working with applications each organization is concerned with the following:

- No illegal or fake applications are installed on the client systems.
- Systems are not infected by the use of applications.
- Malware does not spread through applications.
- Unnecessary applications do not clog the systems.

With Application Control, the administrators can authorize or unauthorize the users to access and work with certain applications, so no one accesses an unwanted application. If the users try to access the unauthorized application, a notification may 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 applicable only for the clients with Windows operating systems.

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

1. Log in to Thirtyseven4 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**

With Custom, you can customize the setting about what applications you want or do not want to authorize.

If you authorize an application category, all the applications that are displayed in the list of applications are allowed. Likewise if you unauthorize an application category, all the applications that are displayed in the list of applications are blocked.

Using Custom, you can authorize certain applications while unauthorizing other applications from the same application category as per your requirement. 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.

*Make sure 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**

With Add Application, you can add a new application to the default list. Adding and unauthorizing of an application or file that belongs to operating system or other system specific application may cause system malfunction. So you are advised to add an application that is not a part of operating system or other system application.

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 Thirtyseven4 improve the quality of the software product.*

*You can also submit the application metadata to the Thirtyseven4 lab.*

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

### ***Submit Application metadata to Thirtyseven4 Lab***

With the Submit Application metadata to Thirtyseven4 Lab option, you can send metadata of an application to the Thirtyseven4 lab to include it in the application categories.

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

However in case you have unauthorized an application category but an application is not yet blocked from being run on a system, you can submit that application. Thirtyseven4 analyzes the application and then enlists it in the category.

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.

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 its Application Metadata to the Thirtyseven4 lab.

## **Device Control**

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

- No malware is installed on the client systems
- Autorun feature does not activate any infection
- No malware is transferred from one system to the other
- Unnecessary data or applications do not clog the systems

With Device Control, the administrators can create policies with varying rights. For example, administrators can block complete access to removable devices, give Read only and no write access so nothing can be written on the external devices, and customize access to admin configured devices. Once you apply the policy to a group, the access rights are also applied.



The Device Control feature is applicable only for the clients with Windows operating systems.

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

1. Log in to Thirtyseven4 Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **Device Control**.
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 Thirtyseven4 Endpoint Security 5.2 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 - 85.

## Update Settings

Imagine a work environment where a large number of systems are installed. The updates to security product may be available regularly and the administrators face the challenge to update all the client systems so that the security product is up to date and the entire environment is secure from the latest threats.

The Update Settings feature of Thirtyseven4 empowers you to create policies for taking the updates automatically for all the clients from various sources. For example, the updates can be downloaded directly from the Internet, from Endpoint Security Console, or specified update servers. This way you can take the updates from different servers and reduce the load on a single server.

The following table shows a comparison of the features in Update Settings that are applicable for different Thirtyseven4 Endpoint Security clients on different operating systems:

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

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

1. Log in to Thirtyseven4 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 Servers

For creating different policies, you may select different options for Update Mode.

If you select Download from Specified Update Servers , you should enter update server locations in the list.

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

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

If you select the Download from Specified Updates Servers option, you are advised to enter 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 updates from these locations in Client Settings.

To enter a server location, follow these steps:

1. On the Thirtyseven4 Endpoint Security Dashboard, click **Home**.
2. On the Home screen, 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**

With Internet Settings, the administrators have 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, Messenger etc. get the Internet connection. This is very helpful in allowing the client modules to function in a secure work environment when default Internet connection is not allowed.

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

1. Log in to Thirtyseven4 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 Sever, type the sever name.

6. In Port, type the port number.

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

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

## General Settings

With General Settings, you can create a policy that authorizes the clients to access the client setting 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 Thirtyseven4 Endpoint Security clients on different operating systems:

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

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

1. Log in to Thirtyseven4 Endpoint Security web console and then click the **Settings** tab.
2. On the Settings screen, click **General Settings**.
3. To give access to the client settings, select **Authorize access to the client settings\***.

*Password setting is activated.*

4. 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.*

5. To activate self protection, select **Enable Self Protection\***.
6. To get the news alert about various incidents, select **Enable News alert\***.
7. To save your setting, click **Save Policy**.



To know for which clients the asterisked features are applicable, refer to the [comparison table](#) at page, 76.

## Schedule Settings

Scanning regularly keeps the systems clean and protected. In an organization where the client systems may be installed in physically separate environments, it is important that there is a policy through which the administrator can centrally control about how to scan all the systems and when to initiate scanning as the systems may be busy with their own tasks.

You can schedule scanning for the following.

### Client Scan

With Client Scan, you can create policies to initiate scanning the clients automatically at time and intervals based on their requirement. You can define whether the scan should run daily or weekly, select scan mode (Quick Scan, Thorough Scan), and 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 Thirtyseven4 Endpoint Security clients on different operating systems:

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

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

1. Log in to Thirtyseven4 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**

With Client Schedule Scan, you can define schedules to scan the clients at the preferred 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**

With Scanner Settings, you can define what scan mode you prefer for scanning the clients, what items you want to scan, and so on.

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***

With Antimalware Scan Settings, you can 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 applicable only for the clients with Windows operating system.

### **Application Control**

With Application Control, you can create policies to initiate scanning of the applications installed and authorized and unauthorized applications present on the clients automatically at the preferred time and intervals.

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

1. Log in to Thirtyseven4 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 applicable only for the clients with Windows operating systems.

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

With Application Control Schedule Scan, you can 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***

With Scan and Report, you can initiate scanning of the applications in various ways such as:

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

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

## **Tuneup**

With Tuneup, you can create policies to tune up the clients automatically at the time and intervals preferred.

To create a policy for Tuneup, follow these steps:

1. Log in to Thirtyseven4 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 applicable only for the clients with Windows Desktop operating systems.

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

With Tuneup Schedule Scan, you can 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***

With Tuneup Settings, you can 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

With Server, you can 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 Thirtyseven4 client from computers on network, it is advisable that you password-protect Thirtyseven4 Endpoint Security. Thirtyseven4 Endpoint Security requires you to specify a console password; however, you can modify your password from the Thirtyseven4 Endpoint Security.

To change the console password, follow these steps:

1. Log in to Thirtyseven4 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

With Notification, you can 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, unauthorized device or application trying to access or virus definitions getting 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 – for notification for various incidents.
- Configure Email for Event Notification – for creating a list of Email IDs for sending notification.

### **Email Notification**

To configure Email Notification, follow these steps:

1. Log in to Thirtyseven4 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 Notification.

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

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

*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.
  6. Under **Device Control**, select the mediums through which you want to get the notification for the following incident:
    - Attempt to access unauthorized device

*Note: Under **Application Control**, select the mediums through which you want to get the notification for the following incident:*

    - Attempt to access unauthorized application

7. 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
8. 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
9. Under **Clients**, select the mediums through which you want to get the notification for 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
10. Under **License related**, select the mediums through which you want to get the notification for the following incidents:
  - License expired
  - License is about to expire
  - License limit exceeds
11. To save your setting, click **Apply**.

### **Configuring Email for Event Notification**

To configure Email Event Notification, follow these steps:

1. Log in to Thirtyseven4 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 for Event Notification, click **Configure**.  
*The Email Notification prompt appears.*
4. In the List of Email ID's, type an email address and then click **Add**.  
*You can enter multiple Email IDs.*
5. To save the Email IDs, click **Apply**.
6. To save your setting, click **Apply**.

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

## SMTP Settings

With SMTP Server Settings, you set the SMTP Host Details. All emails from Endpoint Security Server such as Notification mails, Report mails and so on will be sent to the following SMTP Server for further routing:

1. Log in to Thirtyseven4 Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > SMTP Settings**.
3. In SMTP Server text box, type the IP Address or domain name of SMTP server.
4. In Port text box, type the port number.
5. In 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 Password text box, type the password.
7. In the Notify from Email Address text box, type the Email ID. This Email ID is a notification from Email ID and will appear as From Address in all Emails sent from EPS server.
8. To apply your settings, click **Apply**.

## Add Device

With Add Device, you can get the details of removable devices and then add such devices to the Manage Removable Devices list. The devices added here are available 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 in to Thirtyseven4 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 on the System and click **Add** to fetch the details for the Removable devices.  
*The removable devices details include Serial number, Manufacturer, Size, and Device name.*
4. You may 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 may 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

Redirection 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.

To configure Redirection , follow these steps:

1. Log in to Thirtyseven4 Endpoint Security web console and then click the **Admin Settings** tab.
2. On the Admin Settings page, go to **Server > Redirection**.
3. In 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

With Manage Users, you can 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 Thirtyseven4 Endpoint Security. There can only be one user with Super Administrator privileges. A Super Administrator can create, and modify Administrator users. The default username for Super Administrator is 'administrator'.

A user with Super Administrator privileges is the only user who can uninstall Thirtyseven4 Endpoint Security.

### **Administrator**

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

- A user with Administrator privileges cannot create another user with Administrator privileges.
- A user with Administrator privileges cannot uninstall Thirtyseven4 Endpoint Security.

### **Report Viewer**

A user with 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 in to Thirtyseven4 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 in to Thirtyseven4 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 **Edit** 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 in to Thirtyseven4 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 may delete a user if you have the right privileges to do so.*  
*A confirmation message appears.*
4. To delete the users, click **Yes**.

### **General**

With General, you can 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 determined here.

To configure General, follow these steps:

1. Log in to Thirtyseven4 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 may select 20 minutes, 30 minutes, or 60 minutes.*
4. To apply your setting, click **Apply**.

### **Client Installation**

With Client Installation, you can 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 it is required to do so.

In order to change the Thirtyseven4 client installation path, follow these steps:

1. Log in to Thirtyseven4 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 Client Installation feature is applicable only for the clients installed on Windows operating system.

## Inactive Client Settings

When you uninstall the Thirtyseven4 client from a computer, the program automatically notifies the server. When the server receives this notification, it removes the client icon in the computer tree to show that the client does not exist anymore.

However, if the client is removed using other methods, such as reformatting the computer hard drive or deleting the client files manually, Thirtyseven4 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 have the display of active clients protected under Thirtyseven4 Endpoint Security only, you can configure Thirtyseven4 Endpoint Security to automatically remove inactive clients from the computer protection list.

To automatically remove inactive clients, follow these steps:

1. Log in to Thirtyseven4 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 Thirtyseven4 Endpoint Security considers a client is inactive.
5. To apply the setting, click **Apply**.

# Reports

The Reports menu provides 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 gives the last update report of the offline clients. Use these logs to assess your organization's virus protection policies and to identify clients that are at a higher risk of infection. Also use these logs to verify if the clients have the latest updates.

## Clients

With Clients, you can 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

Using Virus Scan, you can generate reports about whether any virus is found upon 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 in to Thirtyseven4 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 form.*

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 may 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

Using AntiMalware Scan, you can generate reports about whether any malware is found upon 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 in to Thirtyseven4 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 form.*

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 may 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

Using Web Security, you can 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 in to Thirtyseven4 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 for may be displayed both in Chart and Tabular form.*

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 may also save the report as CSV or PDF.*

Note: In case of Business flavor of Thirtyseven4 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

Using Tuneup, you can 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 in to Thirtyseven4 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 form.*

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 may 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

Using Device Control, you can generate reports on policies 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 in to Thirtyseven4 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 form.*



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 may 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

Using Application Control, you can generate reports on how many applications were scanned upon access and installation, whether they were authorized or unauthorized applications, by scanning the clients through the Schedule Scan and On Demand Scan (Clients > Client Action > Application Control Scan).

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 in to Thirtyseven4 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 form.*

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 in to Thirtyseven4 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 may 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. Also it includes information of what authorized and unauthorized applications are present on client machine.

## Viewing Reports of IDS/IPS

Using IDS/IPS, you can generate reports on whether Port scanning attack, DDOS (Distributed Denial of Service) attack, or any intrusion was detected, and what actions were taken (Settings > Client Settings > IDS/IPS).

To view reports of IDS/IPS, follow these steps:

1. Log in to Thirtyseven4 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 may 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

Using Firewall, you can 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 in to Thirtyseven4 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 may 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

With Sever, you can check the event logs of all the incidents going on server.

To view the event logs on Server, follow these steps:

1. Log in to Thirtyseven4 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 may 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

With Manage, you can manage the reports generated on server and clients. You can set when the reports can be removed automatically, export the reports, and delete the reports manually.

## Managing Settings

With Settings, you can set when to remove the reports automatically in the following way:

1. Log in to Thirtyseven4 Endpoint Security web console and then click the **Reports** tab.
2. On the Reports page, select **Manage > Settings**.
3. On the Settings page, select 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

With Export, you can export the reports in PDF in the following way:

1. Log in to Thirtyseven4 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 Thirtyseven4 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

With Delete Reports, you can delete the reports manually in the following way:

1. Log in to Thirtyseven4 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 until 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.

# Update Manager

Update Manager is a tool that is used to download and manage the updates for Thirtyseven4 Endpoint Security. It provides you the flexibility to download the updates on a single machine. It also provides the facility of automatically updating Thirtyseven4 Endpoint Security for enhancements or bug fixes. All Thirtyseven4 Endpoint Security clients fetch updates from this centralized location.

Update Manager available within Thirtyseven4 Endpoint Security includes all the features that are available in the Update Manager application. Any change in settings made over here, will reflect in the Update Manager application.

## Update Manager Status

Update Manager Status includes information of all types of updates downloaded by Update Manager. It displays the Version, Service Pack and the Virus Database Date of the Thirtyseven4 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 Thirtyseven4 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 back 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 Thirtyseven4 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 if you want to enable automatic update of Thirtyseven4 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 as per the time interval you specify. This feature is enabled by default and the default value of time interval in the list is 10 days.

To save you settings, click the **Apply** button.

## Alternate Update Managers

In case of big network, you may also deploy multiple Update Managers. This enables load balancing as Clients can take the updates from different servers. You can configure clients to take the updates from these locations in Client Settings.

To configure Alternate Update Managers, follow these steps:

1. Log in to **Thirtyseven4 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.*

# License Manager

With License Manager, you can manage the Thirtyseven4 Endpoint Security license. You can check the status of your Thirtyseven4 Endpoint Security license, add new licenses to your existing setup, renew your license, and update license information.

## Status

With Status, you can check the current status of your license information. To check the status of your license, follow these steps:

1. Log in to **Thirtyseven4 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 Thirtyseven4 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 Thirtyseven4 Endpoint Security. Product.
<b>Product Type</b>	Displays the product type. Example: Regular.
<b>Activation Number</b>	Displays the activation number of Thirtyseven4 Endpoint Security. Activation number is obtained after successful registration of Thirtyseven4 Endpoint Security.
<b>Installation Number</b>	Displays the Installation Number.
<b>License Valid till</b>	Displays expiry date of the Thirtyseven4 Endpoint Security license.
<b>Maximum number of systems under console</b>	Displays total number of systems which can be protected with Thirtyseven4 Endpoint Security.

### **Update License Information**

This feature is useful to synchronize your existing license information with Thirtyseven4 Activation Server. With Update License Information, 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.

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 Thirtyseven4 Support team and provide your Product Key and Renewal Key.

## **License Addition**

With License Addition, you can add new licenses to your existing license. For adding a new license, you need to obtain an additional license key from Thirtyseven4. To obtain an additional license key, you need to fill an order form provided in Thirtyseven4 Endpoint Security and submit it to the Thirtyseven4 team. Once you receive the additional license key, you can add it.

To add a new license, follow these steps:

1. Log in to **Thirtyseven4 Endpoint Security** web console.
2. On the Home page, click the **View License** link.
3. On the License Manager page, click the **License Addition** tab.

*The Product Key and Activation Number are displayed in their respective fields.*

4. In the Additional Key text boxes, type the Additional keys.
5. Click **Submit**.

## **License Renewal**

With License Renewal, you can renew your license any time after activation and within four (4) months after expiry. To renew the license, you need to obtain a renewal key from Thirtyseven4 by filling an order form provided in Thirtyseven4 Endpoint Security and submitting it to the Thirtyseven4 team. Once you receive the renewal key, proceed in the following way:

1. Log in to **Thirtyseven4 Endpoint Security** web console.
2. On the Home page, click the **View License** link.
3. On the License Manager page, click the **License Renewal** tab.

*The Product Key and Activation Number are displayed in their respective fields.*

4. In the Renewal Key text boxes, type the renewal key.
5. Click **Submit**.

## License Order Form

With License Order Form, you can print or email a license order form for additional license or renewal license.

This is an offline activity and only helps you in creating the License information sheet along with the order details. You still need to contact your vendor and place the order for your license requirement. While placing an order for either additional license or renewal license, you should submit the copy of order form which will be generated by filling the form.

1. Log in to **Thirtyseven4 Endpoint Security** web console.
2. On the Home page, click the **View License**.
3. On the License Manager page, click the **License Order Form** tab.
4. To create License Addition form for existing Endpoint Security license, enter the number of additional systems for which additional license is required and then click **Create Order Form**.
5. To create License Renewal form for existing Endpoint Security license select the duration for which you want to renew the license and then click **Create Order Form**.

*An order is created.*

- Take a print-out of the form by clicking the Print button or you may also email the order form to us.
- Sign on the form and send it to your vendor or Thirtyseven4 L.L.C. to process the order.

# Technical Support

Thirtyseven4 provides extensive technical support for registered users. It is recommended that you have all the necessary details with you during the email ([support@thirtyseven4.com](mailto:support@thirtyseven4.com)) or call to receive efficient support from Thirtyseven4 support executives.

## Details that are necessary during the call

- 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 Thirtyseven4 technical support.
- Details: When did the problem first appear? What were you doing when the problem appeared?

## What should I say to the technical support personnel?

You need to be as specific as possible and provide maximum details as the support executive will provide solution based on your input.

## Contact Thirtyseven4 Support Center

Thirtyseven4, L.L.C.  
P.O. Box 1642,  
Medina, Ohio 44258  
United States  
Phone number: 1-877-374-7581  
Fax number: 1-866-561-4983  
Email: [support@thirtyseven4.com](mailto:support@thirtyseven4.com).  
Thirtyseven4 Support: <http://support.thirtyseven4.com>.  
Web: <http://www.thirtyseven4.com>.  
Sales: [sales@thirtyseven4.com](mailto:sales@thirtyseven4.com).