



Thirtyseven4 Endpoint Security 7.2

Administrator's Guide

**TSEPS SME
TSEPS Business
TSEPS Total**

Copyright Information

Copyright © 2017 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 transmitted in any form without prior permission of Thirtyseven4, LLC, P. O. Box 1642, Medina, Ohio 44258.

Marketing, distribution or use by anyone barring the people authorized by Thirtyseven4, LLC is liable to legal prosecution.


Trademarks

Thirtyseven4 and DNAScan are registered trademarks of Thirtyseven4, LLC.

About This Document

This Administrator's 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
Bold Font	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

Chapter 1. Introducing Thirtyseven4 Endpoint Security	1
How Does Thirtyseven4 Endpoint Security Work?	1
New in this release	1
<i>Available flavors</i>	6
Network Deployment Scenarios	7
<i>Scenario 1</i>	7
Network Setup Description	7
Thirtyseven4 Recommendation	8
<i>Scenario 2</i>	8
Network Setup Description	8
Thirtyseven4 Recommendation	9
<i>Scenario 3</i>	9
Network Setup Description	9
Thirtyseven4 Recommendation	10
Chapter 2. Getting Started	11
Prerequisites	11
System Requirements for TSEPS server	11
<i>General requirement</i>	11
<i>Operating system requirement</i>	12
<i>Additional software required for TSEPS server</i>	13
<i>Java Runtime Environment (JRE) requirements</i>	13
System requirements for Thirtyseven4 EPS clients	13
<i>General requirements</i>	13
<i>Operating system requirements</i>	14
<i>System Requirements for Mac OS</i>	15
Installing Thirtyseven4 Endpoint Security on Windows Operating System	15
Enabling IIS on Windows Server 2003 and XP	19
Installing Multiple Thirtyseven4 Endpoint Security Server	19
<i>Upgrading previous version of Thirtyseven4 Endpoint Security to the latest version</i>	19
Chapter 3. Post Installation Tasks	22
Registration	22
<i>Registering Online</i>	22
<i>Internet Settings</i>	22
Reactivation	23
<i>Reactivating Thirtyseven4 Endpoint Security</i>	23
<i>Configuring Update Manager</i>	23
<i>Accessing Update Manager</i>	23
Features of Update Manager	24
Status	24

Configuration	24
Schedule Scan in Update Manager	25
Connection Settings.....	26
Reports	26
Configuring ports on the Azure or AWS Cloud machine	27
Uninstalling Thirtyseven4 Endpoint Security.....	27
Chapter 4. About Thirtyseven4 Endpoint Security Dashboard	29
Log on the Thirtyseven4 Endpoint Security Web console	29
Resetting the Web console password	29
<i>Resetting the Web console password with Forgot Password link.....</i>	<i>30</i>
<i>Resetting the Web console password with Password Reset tool</i>	<i>30</i>
Areas on the web console	31
Dashboard Area.....	32
Overview.....	32
Network Health.....	33
Status	34
Security	34
Compliance.....	35
Assets.....	35
Chapter 5. Clients	36
Client Status tab.....	36
Client Action tab	37
Scan	38
Scan Settings.....	38
Update.....	39
Tuneup	40
Tuneup Settings.....	41
Application Control Scan.....	42
Scan Settings.....	43
Vulnerability Scan.....	43
Data-At-Rest Scan.....	44
Scan Settings.....	44
Patch Scan	45
Patch Install.....	46
Temporary Device Access	48
Chapter 6. Client Deployment	50
Through Active Directory	50
Synchronizing with Active Directory	51
Editing Synchronization	52
Removing Synchronization	52
Exclusion	52
Remote Install	53

<i>Exception Rules:</i>	53
Viewing installation status	55
Notify Install	56
Client Packager.....	57
<i>Creating Windows Thirtyseven4 Client Packager</i>	57
<i>Creating Mac Thirtyseven4 Client Packager</i>	58
<i>Sending the package through email</i>	59
Sending a minimal Client Packager	59
Sending a custom Client Packager	60
Login Script	60
<i>Installing Login Script</i>	60
<i>Opening Login Script Setup</i>	61
<i>Assigning Login Script</i>	61
Installing Thirtyseven4 Endpoint Security on Mac Operating Endpoints	61
Remote Installation of Thirtyseven4 Endpoint Security on Mac System.....	62
<i>Remote installation using Apple Remote Desktop or Casper</i>	62
Creating Client Agent package	63
Installing Client Agent using Apple Remote Desktop or Casper	63
<i>Connecting remotely using Secure Shell</i>	64
Using Terminal (for Mac OS)	64
Using PuTTY (for Windows OS)	65
Installing Thirtyseven4 Mac Client Agent	66
Creating the Mac Thirtyseven4 Client Installer	67
Disk Imaging	67
Firewall Exception Rules	68
Remote Uninstall	68
<i>Stop Uninstallation Notifications</i>	69
Chapter 7. Manage Groups	70
Adding a Group	70
Adding a Subgroup	70
Deleting a Group	71
Renaming a Group	71
Importing from Active Directory	72
Setting Policy to a Group.....	72
Changing Group of an Endpoint	73
Exporting groups and policies	73
Importing groups and policies.....	73
Chapter 8. Manage Policies	75
Understanding Security Policy Scenario	75
Creating Policies	77
<i>Creating a new policy</i>	77

<i>Copying a policy</i>	77
<i>Renaming a policy</i>	77
<i>Deleting a policy</i>	78
<i>Importing and Exporting Policies</i>	78
Exporting a policy	78
Importing a policy	78
Chapter 9. Assets	80
Viewing the details for Endpoints	80
<i>Enabling Asset Management</i>	81
Chapter 10. Settings	82
Client Settings	82
<i>Scan Settings</i>	82
Scanner Settings	83
Virus Protection Settings	84
Advanced DNAScan Settings	84
Block suspicious packed files	85
Automatic Rogueware Scan Settings	85
Disconnect Infected Endpoints from the network	85
Exclude Files and Folders	86
Exclude Extensions	87
<i>Email Settings</i>	87
Email Protection	87
Trusted Email Clients Protection	88
Spam Protection	89
<i>External Drives Settings</i>	91
External Drives Settings	91
Autorun Protection Settings	91
Mobile Scan Settings	91
<i>Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)</i>	92
<i>Firewall</i>	94
<i>Web Security</i>	98
Browsing Protection Settings	99
Phishing Protection Settings	100
Web Categories	100
<i>Application Control</i>	102
<i>Advanced Device Control</i>	104
To create a policy for Advanced Device Control, follow these steps:	104
Adding exceptions to the device control list	106
Adding Device to Server	107
<i>Data Loss Prevention</i>	107
Preventing leakage of data	108
<i>File Activity Monitor</i>	110
Enabling File Activity Monitor	110
<i>Update Settings</i>	111

<i>Internet Settings</i>	112
<i>Patch Server</i>	113
<i>General Settings</i>	113
Schedule Settings	114
<i>Client Scan</i>	114
Client Schedule Scan.....	115
Scanner Settings	115
Antimalware Scan Settings	116
<i>Application Control</i>	116
Application Control Schedule Scan.....	117
Scan and Report.....	117
<i>Tuneup</i>	117
Tuneup Schedule Scan.....	117
Tuneup Settings.....	118
<i>Vulnerability Scan</i>	118
Scheduling Vulnerability Scan	118
Scan and Report.....	119
<i>Data-At-Rest Scan</i>	119
<i>Patch Scan</i>	119
Chapter 11. Reports	121
Client.....	121
<i>Viewing Reports of Virus Scan</i>	121
<i>Viewing Reports of AntiMalware Scan</i>	122
<i>Viewing Reports of Web Security</i>	123
<i>Viewing Reports of Tuneup</i>	124
<i>Viewing Reports of Advanced Device Control</i>	124
<i>Viewing Reports for Data Loss Prevention (DLP)</i>	125
On Access Scan	125
On Demand/Schedule Scan	127
<i>Viewing Reports for Application Control</i>	128
<i>Viewing Reports of IDS/IPS</i>	130
<i>Viewing Reports of Firewall</i>	131
<i>Viewing Reports of Wi-Fi</i>	132
<i>Viewing Reports of Vulnerability Scan</i>	133
<i>Viewing Reports for File Activity Monitor</i>	134
Viewing reports for file activity	134
<i>Viewing Reports for Asset Management</i>	135
Viewing reports for asset management.....	135
Asset Incidents	135
Current Assets	136
<i>Viewing Reports of Patch Management</i>	136
Server	138
Manage	139

<i>Managing Settings</i>	139
Managing Export.....	139
Managing Delete Reports	139
Chapter 12. Admin Settings	141
Server	141
<i>Change Password</i>	141
<i>Change Email Address</i>	141
<i>Notification</i>	141
Email Notification	142
<i>SMTP Settings</i>	144
<i>Manage Devices</i>	145
Cleaning USB device	145
Adding exceptions to the device control policy	147
<i>Data Loss Prevention</i>	148
User Defined Dictionary	148
Domain Exceptions	149
Custom Extensions	150
Application Exceptions.....	152
Network share Exception	153
<i>Redirection</i>	154
<i>Manage Users</i>	155
Super Administrator	155
Administrator.....	155
Report Viewer	156
Creating New Users.....	156
Modifying Existing Users.....	156
Deleting Users	157
<i>Internet Settings</i>	157
<i>Patch Management</i>	157
Installing Patch Server:	157
Adding New Patch Server.....	158
Removing Patch Server	158
Configuring Patch Server.....	159
<i>General</i>	161
Multiserver Migration Period	162
Clients	162
<i>Client Installation</i>	162
<i>Inactive Client Settings</i>	163
<i>Asset Management</i>	163
<i>Roaming Clients</i>	163
Reinstallation	164
<i>Data Loss Prevention (DLP)</i>	165
Enabling DLP feature.....	165
Chapter 13. Update Manager	167

Viewing Update Manager Status	167
Update Manager Settings.....	168
<i>Update Manager Schedule</i>	168
Alternate Update Managers.....	169
<i>Adding New Alternate Update Manager</i>	169
<i>Viewing details of Alternate Update Mangers</i>	169
<i>Modifying Existing Alternate Update Manager details</i>	171
<i>Alternate Update Manager Schedule</i>	171
<i>Deleting Alternate Update Manager</i>	172
Chapter 14. License Manager	173
Status.....	173
<i>Update License Information</i>	173
<i>View license history</i>	174
License Order Form	174
<i>Renew my license</i>	175
<i>Add license for new endpoints</i>	175
<i>Buy additional feature</i>	176
<i>Edition Upgrade</i>	176
Chapter 15. Patch Management.....	178
Workflow of Patch Management.....	178
System requirements for Patch Management server	178
Installing Patch Management server on Windows Operating System	178
Back up the patch server data.....	180
Offline Patch Synchronizer	180
Patch Server Control Panel	181
Uninstalling patch server	182
Chapter 16. Technical Support	183
Support	183
Web Support.....	183
Email Support	183
Live Chat Support	183
Phone Support.....	183
Remote Support.....	183
<i>If the Product Key is Lost</i>	184
Contact Thirtyseven4 Support Center	184

Introducing Thirtyseven4 Endpoint Security

For every organization, security of valuable data and resources is of paramount concern. Today Web technology is an integral part of business processes for all organizations. This puts them more at risk from new and unknown threats and attacks. 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, spyware, riskware, adult content, and hackers.

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

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. For a detailed description of console and client agent system requirements and compatibilities, see [System Requirements](#).

TSEPS helps the administrators 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 from any workstation(s), it reinstalls Thirtyseven4 remotely without user intervention. This keeps the computers and the network safe from virus threats.

New in this release

Thirtyseven4 Endpoint Security 7.2 brings you the following:

- You can install Thirtyseven4 EPS server on Azure or AWS cloud server also. This is called Public Installation.
- Client Packager
In the Mixed mode installation, the client packager method is changed.

The client packager gives you an additional option to enter alternate/public/natted IP address or domain name for remote client deployment.

This server (deployed on internal/local IP but natted to public IP/FQDN) has local and remote clients.

- Redirection
 - In case of software version upgrade, the previous version TSEPS Client will get uninstalled and new version of TSEPS client will get installed.
 - The Redirection page gives you an option to provide public/natted IP address or server name.

The following table explains the supported redirection cases,

TSEPS Server of earlier version	TSEPS Server of higher version
Installed on local/private IP	Installed on local/private IP
Installed on local/private IP	Installed on local/private Domain
Installed on local IP (natted with public)	Installed on local IP (natted with public)
Installed on public IP	Installed on public IP
Installed on public IP	Installed on FQDN(Fully qualified Domain Name)

- Patch Management
 - Configuration of Patch Management Server in Distributed TSEPS environment.
For the remote clients, install the Patch Server in the network where the remote clients are deployed. The private IP of the Patch server should be natted to public IP.
 - Multiple endpoints can be added to exclusion list for patch management.
 - Patch Management supports the following applications along with Microsoft applications,
 - VideoLAN Player
 - Adobe Acrobat
 - Adobe Flash Player
 - Adobe Reader
 - puTTY
 - Notepad++
 - Java
 - 7-zip compression Tool
 - Mozilla Thunderbird
 - Mozilla Firefox
 - You can create an offline Patch Repository. With the Thirtyseven4 offline Patch synchronizer wizard, you can create an offline patch repository from the

Thirtyseven4 Patch Server and synchronize the Thirtyseven4 patch server from the Offline Patch Repository.

- The Patch Management - client-wise report page displays the following patch details:
 - Scanned Patches - Displays the details of scanned patches.
 - Patch Downloaded - Displays the details of downloaded patches.
 - Installed Patches - Displays the details of installed patches.
 - Installation Failed - Displays the details of failed installation of patches.
- In this release, Patch Server Control Panel is incorporated. You can view the status of patch management services with the help of Patch Server Control Panel. This view is used for troubleshooting purpose. To ensure that all the services are in running state for smooth functioning of the patch management server. You can also delete patch metadata and its content which are or of older version and patch server does not need this data in future.
- Asset Management
 - Customized reports for Asset Management.
 - A Product key will be displayed for Windows OS. This is supported on Windows Vista and above OS.
 - A Product key will be displayed for MS Office. This is supported for MS Office 2010 to 2016.
 - License status of MS Office installed will be displayed as Unlicensed / Licensed / OOBGrace / OOTGrace/ NonGenuineGrace / Notification / ExtendedGrace.
- Reports
 - In the Reports section, you can generate user wise reports of all the incidents happening on the endpoints.
 - The 'User Name' field is added for the following modules in the client reports section:
 - Virus Scan
 - Web Security
 - IPS
 - Application Control (On Access)
 - Advance device control
 - Data Loss Prevention (On access & On Demand)
 - File Activity Monitor
 - Vulnerability Scan
 - Asset Management

This feature is available in the clients with Windows and Mac operating systems.

- In the exported client status report (Clients>Client Status), **Last Connected On** column is added. Now the Administrator can know when the client was last time connected to the TSEPS Console.
- Admin will receive reports and notification for ransomware incidents occurred at the endpoints. Ransomware detected on endpoints can be configured from Admin Settings > Email Notification.
- Data Loss Prevention
 - The following DLP Features are added:
 - DLP for specific group
 - Custom Extension
 - Domain Exception
 - Application Exception
 - Network Share Exception

Domain Exceptions supports only the Outlook and Thunderbird email clients on the Windows platform.
 - Custom Extensions, Application Exception and Network Share Exception are supported on the Windows platform.
 - When the Print Screen option is used to save the screenshot, the DLP feature monitors the action by displaying the pop up and generates a report.
 - DLP data will be monitored only when the data is sent from the local drive to the Network share or to the removable drive and vice versa will not be monitored.
 - DLP enhancements for new detections - Pin Code, Aadhar Number and Vehicle Registration Number fields are added in the report.
 - Mail scanning over SSL for DLP detection support for mail body and mail subject for other mail clients.
- Automatic Site Creation of Standalone Update Manager(STUM)
 - IIS will be installed automatically during the Standalone Update Manager installation process if not installed on the system.
 - The IIS site will be configured on the HTTP protocol.
 - For Windows XP and 2003 OS, IIS should be installed manually and configured on port 80.
 - Standalone Update Manager is not supported on Windows Home Editions.
 - On TSEPS Console, STUM update URL will be fetched if installed with client agent.
 - Automatic and Custom scheduler can be configured for Update Manager.
- Update Manager
 - Update Manager Bandwidth control – Bandwidth range can be given from 64kbps-8192kbps.

- Mirroring Logic is introduced in the Update Manager feature. This download applicable definition files from the update server if these files are missing or corrupt in the Update directory.
- From the TSEPS Console, the following Update Manager settings are also manageable:
 - Service Pack download
 - Schedule Settings
 - Bandwidth Settings
 - Platform list to download the updates
- License related changes
 - DLP pack can be assigned to specific endpoints.
 - DLP count can be added through activation, renewal, additional, addpack transaction.
 - DLP count can be decreased through Renewal transaction.
 - DLP feature can be removed or DLP count can be decreased through Renewal transaction.
 - DLP for specific endpoint will be applicable only from TSEPS version 7.2.
 - If 'TSEPS 7.0 and below product key' with DLP pack is activated/reactivated to TSEPS 7.2 then DLP feature count will be same as the total number of clients.
 - If TSEPS 7.2 product key with DLP to specific endpoint is activated/reactivated to TSEPS 7.0 and below versions then DLP feature count will be same as the total number of clients.
- Reset web console password
 - A 'forgot Password' link is added on the TSEPS Console login page. You can use the link for resetting the web console password.
 - If SMTP settings are not configured, user can reset the password using password reset tool. The password reset tool is located at install location.
 - Number of login attempts allowed are limited to 6. After 6 unsuccessful attempts, the user account will be locked for 6 hours.
- Email protection
 - Email protection supports scanning of encrypted messages sent over POP3 secure socket connection (SSL) protocol.
 - Provision to control Attachment Control Settings – you can block certain type of attachments, emails crafted to exploit vulnerabilities and block attachments with multiple extensions.
 - More number of Email IDs in Notification settings. Now you can add 50 email ids in the notification settings.
 - The **User Name** field is added in the Email notification of the following modules:
 - Virus Scan
 - Application control on access

- Device Control
- Data Leak Prevention
- Asset Management
- Intrusion Prevention
- In Email notifications Endpoint Name, Domain Name, IP Address, date and time are displayed wherever applicable.
- Provision to schedule Internet Access - In Web Security, provision to 'Schedule Internet Access' is provided. At endpoint level, internet access can be blocked/allowed as per the policy settings.
- Windows 2016 server support added for the TSEPS client.
- In the Manages Devices section, **Encryption Status** column is added in the list of devices. This helps to identify encrypted devices. If the devices are encrypted, you can know the encryption type of devices (Not encrypted/Partial/Full). This is applicable for devices added using USB Device method.
- Provision to enable/disable Backup feature. This feature automatically and periodically (multiple times a day) takes a backup of all your important and confidential files present on the endpoint. If you update any file then this feature automatically takes backup of the latest copy.
- Default application list in Application Control is updated.
- Select multiple endpoint at a time to remove the offline clients.
- Thirtyseven4 Endpoint Security installer file type is changed from zip to exe.

Available flavors

Thirtyseven4 Endpoint security is available in the following flavors:

- SME (Small and Medium Enterprises Edition)
- Business
- Total

The following table lists the features that are available in the flavors:

Features	Status		
	SME	Business	Total
Antivirus	✓	✓	✓
Email Protection	✓	✓	✓
IDS/IPS Protection	✓	✓	✓
Firewall	✓	✓	✓
Phishing Protection	✓	✓	✓
Browsing Protection	✓	✓	✓
Vulnerability Scan (VS)	✓	✓	✓

Asset Management	X	✓	✓
Spam Protection	X	✓	✓
Web Security	X	✓	✓
Advanced Device Control	X	✓	✓
Application Control	X	X	✓
Patch Management - Basic	X	X	✓
Tuneup	X	X	✓
File Activity Monitor(FAM)	X	X	✓
DLP	X	X	X

Feature Pack Definition:

Pack Name	Features	Flavor
DLP	Data Loss Prevention + Data-At-Rest Scan	Business and Total edition can subscribe DLP feature. SME need to upgrade to Business or Total to subscribe for DLP.

Network Deployment Scenarios

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

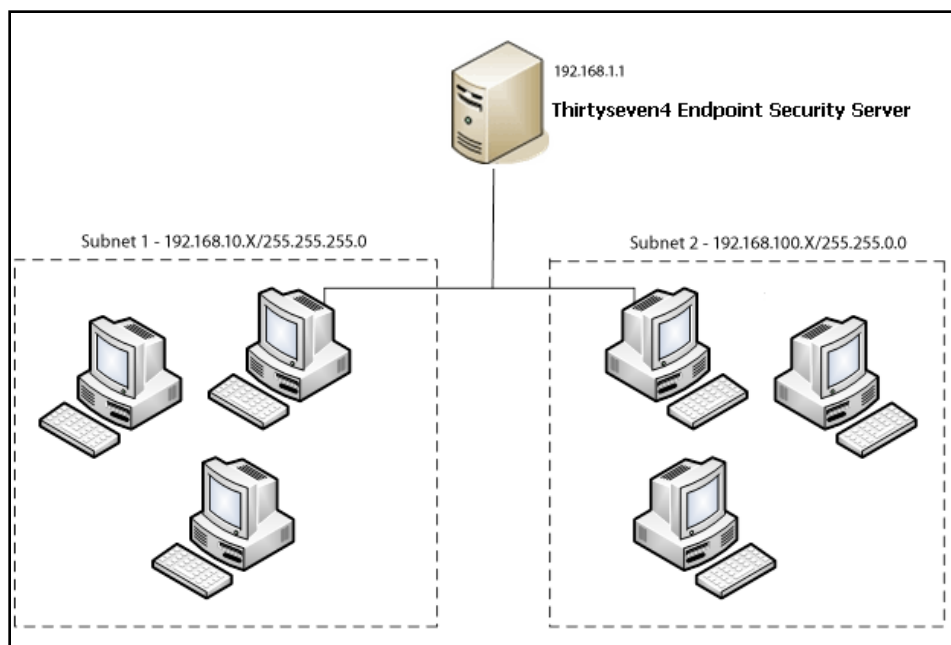
Thirtyseven4 realizes the challenges of varying network setups in different organizations. Therefore, we have provided recommendation for three prominent network setups below:

Scenario 1

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 is installed on the server and Thirtyseven4 client agents are deployed on the endpoint systems in the subnet.



Thirtyseven4 Recommendation

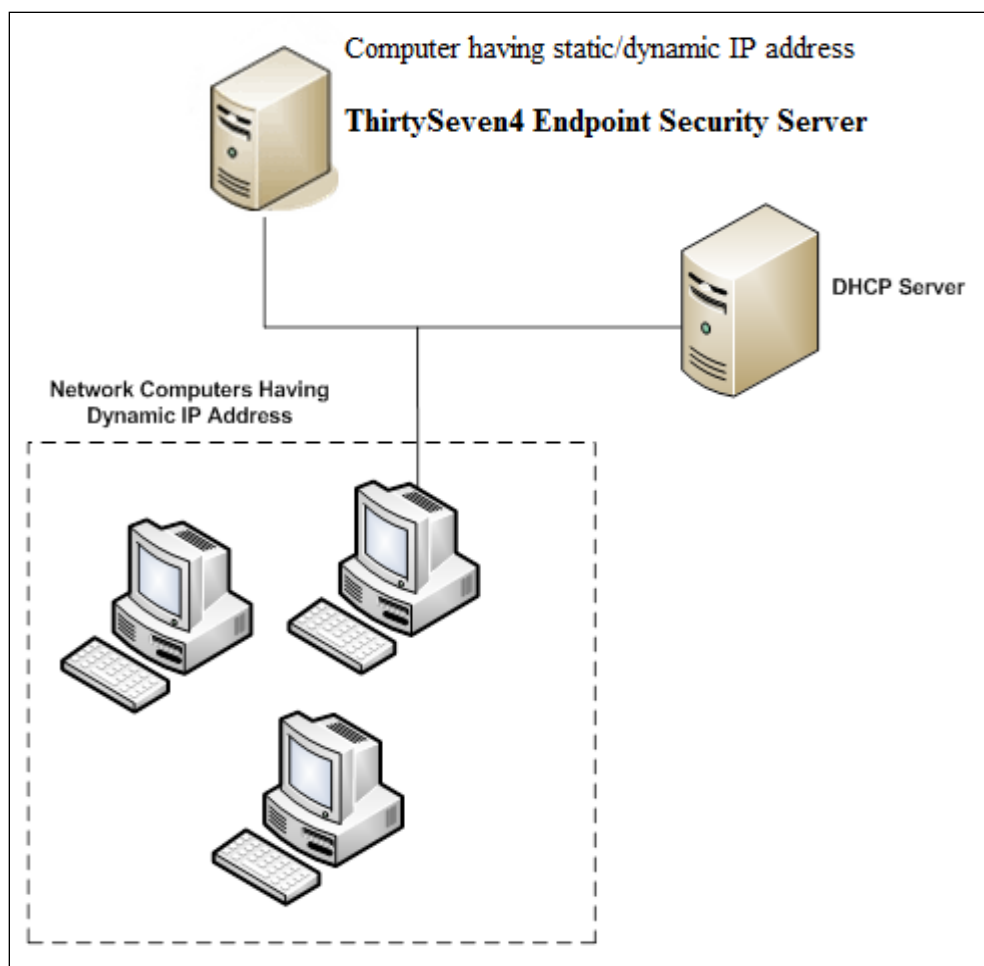
- Before installation, ensure that the server and endpoints are connected. Verify this by pinging server to the endpoints and vice versa.
- The server system should be configured using static IP address.
- During installation of Thirtyseven4 Endpoint Security, select IP Address in the Server Information screen.

Scenario 2

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

Network Setup Description

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



Thirtyseven4 Recommendation

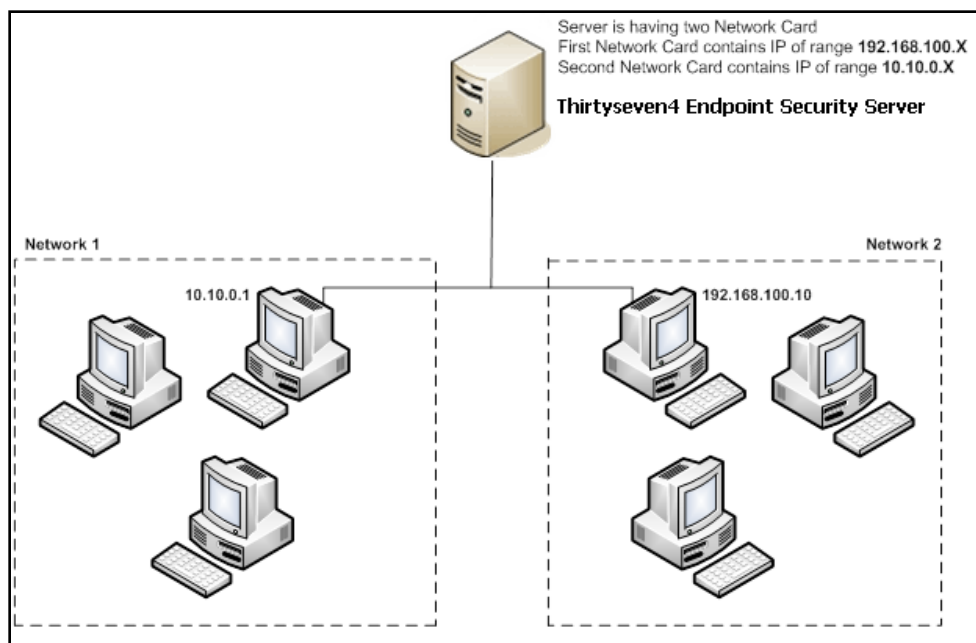
- Before installation, ensure that the server and endpoints are connected. Verify this by pinging server to the endpoints and vice versa.
- The server system and the DHCP server system should be configured using static IP address.
- During installation of Thirtyseven4 Endpoint Security, select an IP address listed in the Server Information screen.

Scenario 3

Installing Thirtyseven4 Endpoint Security on a server using two network cards.

Network Setup Description

The server consists of two network cards, each catering to a network of different IP ranges (Example: 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 is installed on the server with two network cards and Thirtyseven4 endpoints are installed on all endpoint systems of both the networks.



Thirtyseven4 Recommendation

- Before installation, ensure that the server and endpoints are connected. Verify this by pinging server to the endpoints and vice versa. Try to ping using IP address and computer name.
- The server system should be configured using static IP address.
- During installation of Thirtyseven4 Endpoint Security, select Domain Name in Server Information screen. Provide the target server domain name. You can also use Fully Qualified Domain Name (FQDN) of the server if the endpoint has access to a DNS server, which can resolve the FQDN with the endpoint's IP address.

Chapter 2. **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:

- Remove any other antivirus software/hardware from your server and endpoints before installing Thirtyseven4 EPS. A computer system with multiple antivirus programs installed may result in system malfunction.
- Close all open programs before proceeding with installing TSEPS.
- Network should be configured with TCP/IP protocols.
- File and printer sharing for Microsoft Networks must be installed.
- To install on the server, you must have administrator or domain administrator rights.
- To use the Login Script setup, Windows Server 2012 R2 / Windows Server 2012 / Windows 2008 Server R2 / Windows 2008 Server / Windows 2003 Server / Windows 2000 Advanced Server / Windows 2000 Server should be properly configured with Active Directory services.

System Requirements for TSEPS server

System requirements for Thirtyseven4 Endpoint Security server are as follows:

General requirement

The computer where TSEPS server is to be installed must meet the following requirements.

Component	Requirements
Processor	Minimum: 1 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium Recommended: 2 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium or higher
RAM	Minimum: 2 GB Recommended: 4 GB or more
Hard disk space	Minimum: 4800 MB free disk space Recommended: 10000 MB free disk space
Web Browser	<ul style="list-style-type: none"> • Internet Explorer 7, 8, 9, 10, or 11 • Google Chrome 45, 46, or 47 • Mozilla Firefox 38, 39, or 40
Display	1024 x 768



- For more than 25 clients, we recommend to install TSEPS Server and Patch Management server on the Windows Server operating system.
- For more than 500 clients, we recommend a dedicated Web server (IIS).

Operating system requirement

- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 7 Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows Vista
- Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows XP 32-bit SP3, 64-bit SP1 and SP2 / Professional Edition (32-bit / 64-bit)
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)

- Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)

Additional software required for TSEPS server

Thirtyseven4 EPS server needs to have Microsoft IIS Web server as well as Microsoft .NET Framework 4.0 on your computer system.

Web server	Requirements
IIS	IIS Version 10 on Windows 10
	IIS Version 8.5 on Windows 8.1 and Windows Server 2012 R2
	IIS Version 8.0 on Windows 8 and Windows Server 2012
	IIS Version 7.5 on Windows 7 and Windows Server 2008 R2
	IIS Version 7.0 on Windows Vista and Windows Server 2008
	IIS Version 6.0 on Windows Server 2003
	IIS Version 5.1 on Windows XP SP3



The TSEPS installer will install required IIS Components.

Java Runtime Environment (JRE) requirements

Java Runtime Environment (JRE) required to perform installation through Web page and Add Device functionalities are as follows:

OS versions	Requirements	JRE
32-bit	32-bit	JRE 7, JRE 8
64-bit	32-bit	32-bit JRE 7, 32-bit JRE 8
	64-bit	64-bit JRE 7, 64-bit JRE 8

System requirements for Thirtyseven4 EPS clients

System requirements for Thirtyseven4 Endpoint Security clients are as follows:

General requirements

The computer where TSEPS client is to be installed must meet the following requirements.

Component	Requirements
Processor	Minimum: 1 GHz 32-bit (x86) or 64-bit (x64) processor for Windows Vista Recommended: 2 GHz 32-bit (x86) or 64-bit (x64) processor for Windows Vista or higher
RAM	Minimum: 1 GB Recommended: 2 GB or more
Hard disk space	3200 MB
Web Browser	Internet Explorer 5.5 or later

Operating system requirements

Thirtyseven4 Endpoint Security client can be installed on a computer system with any one of the following operating systems:

- Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- Microsoft Windows 7 Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows Vista Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit / 64-bit)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- Microsoft Windows SBS 2011 Standard / Essentials
- Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)
- Microsoft Windows 2000 SP 4 Professional / Server / Advanced Server

System Requirements for Mac OS

Component	Requirements
MAC OS	Mac OS OS X, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11 and 10.12
Processor	Intel or compatible
RAM	Minimum: 512 MB Recommended: 2 GB or more
Hard disk space	1200 MB

To check for the latest system requirements, visit www.thirtyseven4.com.

Installing Thirtyseven4 Endpoint Security on Windows Operating System

To begin installation of Thirtyseven4 Endpoint Security, follow these steps:

1. Download and execute 374eps.exe for Thirtyseven4 Endpoint Security from the URL mentioned in the Software License Certificate.
2. The TSEPS setup wizard starts.
3. Read the information about Thirtyseven4 Endpoint Security. Click **Next**.
4. The license agreement appears. Read the License Agreement carefully. Installation and usage of Thirtyseven4 Endpoint Security is subject to your formal acceptance of the Thirtyseven4 Endpoint Security end-user license terms and conditions.

Select **I Agree** to accept the license agreement, and then click **Next**.

5. Thirtyseven4 EPS server needs Microsoft .NET Framework 4.0 and Microsoft IIS Web server on your computer system to complete the installation.

If .NET and IIS are both already installed, TSEPS setup wizard continues.

*If .NET, IIS or any one of the required components is not installed, a Pre-requisites Checks screen is displayed. The screen shows the installed and missing components that are required to proceed with the installation. Click **Next**.*

The wizard helps you to install .NET and, then IIS component.

To install .NET Framework, follow these steps,

A screen is displayed to install .NET Framework.

- i. Click **Next** to continue with the installation of .NET Framework.
- ii. In the Microsoft .NET Framework 4 Setup screen, select the **I have read and accept the license terms** check box and click **Install**.

Installation progresses.

- iii. In the Microsoft .NET Framework 4 Setup screen, click **Finish**.

- iv. Restart the system.
- v. Start the Thirtyseven4 Endpoint Security installation again with the installer file.

To install IIS, follow these steps,

- i. A screen is displayed to install IIS.

In the Prerequisite – Internet Information Services (IIS) screen, click **Next**.

IIS will be configured on the system.

- ii. Click **Next** to continue the SEPS setup wizard.

If you want to enable IIS on Windows Server 2003 and XP, see Enabling IIS on Windows Server 2003 and XP.

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

The Thirtyseven4 Endpoint Security installer scans system memory for virus infection and verify the installed system components.

While installing Thirtyseven4 EPS, if another antivirus software is already present on your computer, a message appears to uninstall the other antivirus software.

Thirtyseven4 EPS Server installation does not proceed further until you remove the other installed antivirus software.

- 7. On the server information screen, do the following:

- i. In the Server Information section, select one of the following and provide the information:

Domain Name: Select the server **Domain Name** from the list. You can also use Fully Qualified Domain Name (FQDN) of the server if the endpoint has access to a DNS server, which can resolve the FQDN with the endpoint IP address.

If your network is configured using DHCP, select Domain Name.

IP address: Select the IP Address of the server from the list.

- ii. Select the Public Installation check box if you are installing Thirtyseven4 Endpoint Security on a system hosted on the AWS/Azure platforms.

Recommendation

- If you are planning to deploy the endpoints locally (Private), we recommend to do Installation on private IP.
- If you are planning to deploy some endpoint locally and some endpoints remotely, then we recommend do installation on private IP natted to Public IP. In this case while creating a client packager for the remote client, provide alternate IP address or Domain name.
- If you are planning to deploy all the endpoints remotely, we recommend Public Installation.

- iii. In the HTTP section, Port number appears. HTTP Port Number is a port to use as the server listening port. Thirtyseven4 Endpoint Security server address is as follows to launch the console,
 - For Windows XP: http://{ Thirtyseven4_Endpoint_Security_Server_name }/qhscan72
 - For other OS: http://{ Thirtyseven4_Endpoint_Security_Server_name }:{port number}
- iv. In the SSL section, by default the Enable Secure Socket Layer check box is selected and SSL Port number appears.

This port number serves as a listening port for the server. Thirtyseven4 Endpoint Security server address is as follows to launch the console,

- For Windows XP: https://{ Thirtyseven4_Endpoint_Security_Server_name }/qhscan72
- For other OS: https://{ Thirtyseven4_Endpoint_Security_Server_name }:{port number}



Do not use the following ports,

- Port Numbers 0-1023
- MySQL port 62222

- v. Click **Next**.

A message appears for your verification about the Web server settings.

8. To confirm, click **Yes**.

You can make changes in your settings if required.

9. If you select Public Installation, provide the domain name or IP address of the target Server which will be used by the remote clients to communicate with the TSEPS Server.

By default, clients that are installed by the client packager are configured to communicate with the TSEPS server with this domain name/IP address.

10. Click **Next**.

11. The Proxy Settings screen appears.

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

The Thirtyseven4 Endpoint Security modules, Registration Wizard, Update Manager, and Messenger uses the following settings to connect to the internet/

To enable and configure proxy settings:

- i. Select **Enable Proxy Settings**.
- ii. Select the Proxy Type as HTTP Proxy, Socks V 4 or SOCKS V 5 as per your settings
- iii. In the **Proxy Server** text box, type the IP address of the proxy server or domain name (For example, proxy.yourcompany.com).

- iv. In the **Port** text box, type the port number of the proxy server (For example: 80).
- v. In the **User name** and **Password** text boxes, type in your server credentials.
- vi. Click **Next**.

12. The Client Installation Settings screen appears.

Thirtyseven4 client will be installed on the endpoint/workstation as per the path specified in this screen. The following settings are displayed:

- Default endpoint installation path appears. The Path can be provided using either %PROGRAMFILES% or %BOOTDRIVE% variable. For example:
%PROGRAMFILES%\Thirtyseven4\Thirtyseven4 or
%BOOTDRIVE%\Thirtyseven4.
- The Client Agent Communication Port number appears.

The Thirtyseven4 clients communicates with server to fetch important instructions such as scanning and updates, and submit the log to Endpoint Security Server using this port number, so ensure that this port number is not used by any other application in the network.

Click **Next**.

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

To confirm, click **Yes**.

14. The Authentication screen appears.

Create Thirtyseven4 Endpoint Security Administrator password to access the Web console and endpoint password to access the endpoint settings at the endpoint side. The password for administrator and endpoint should be different; else the installation will not proceed.

- i. In the Endpoint Security Administrator Password section, type in your password in the **Password** and **Confirm password** text boxes.
- ii. In the Client Password section, type in your password in the **Password** and **Confirm password** text boxes.

This helps prevent unauthorized users from accessing the Web console and make changes in your settings or remove the endpoints.

- iii. Click **Next**.

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

15. Click **Next**.

A confirmation dialog box 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.

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

The installation starts. The Read me information screen appears. Read the important information related to Thirtyseven4 Endpoint Security.

17. Click **Next**.

18. To register **Thirtyseven4 Endpoint Security** and configure **Update Manager**, click **Next**. If you want to perform these tasks later, clear these options.
19. To complete the installation, click **Finish**.

Enabling IIS on Windows Server 2003 and XP

1. Click **Start> Settings >Control Panel**.
2. In Control Panel, double-click **Add or Remove Programs**.
3. In the Add or Remove Programs dialog box, in the left pane, click **Add/Remove Windows Components**.
4. In the Windows Components page, in the Components box, click Application Server/Internet Information Services (IIS), and then click **Next**.
5. Wait for the installation to complete and close the wizard.



For IIS Installation on windows Server 2003 and Windows XP, you may need OS installation CD.

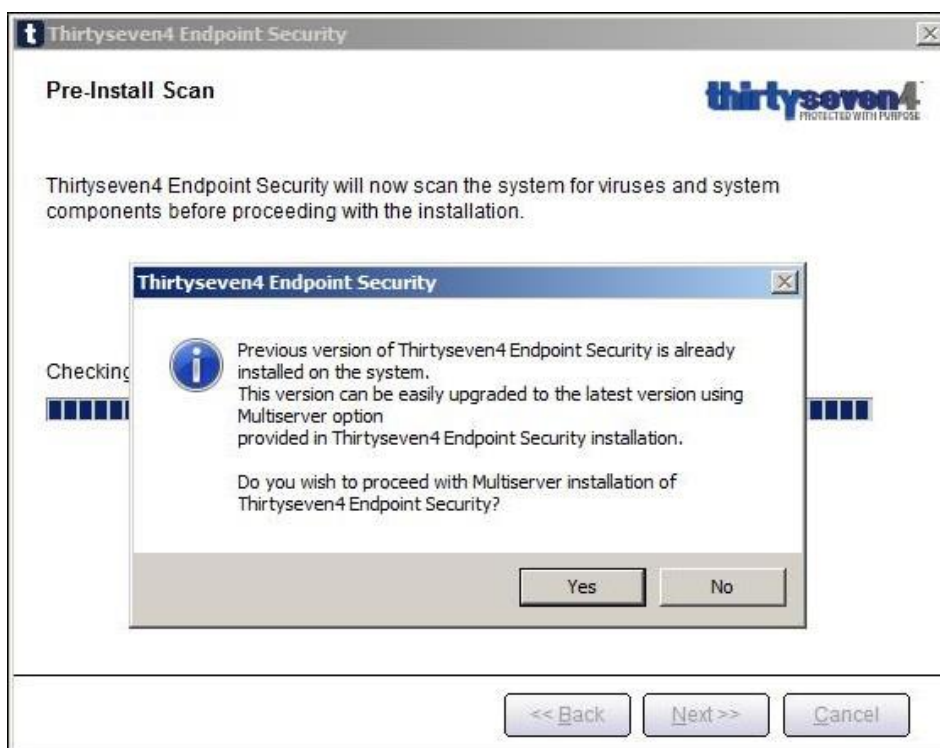
Installing Multiple Thirtyseven4 Endpoint Security Server

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 versions are already installed. This feature enables the administrators to easily migrate to the latest version of Thirtyseven4 Endpoint Security in simple ways.

Upgrading previous version of Thirtyseven4 Endpoint Security to the 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:



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

After the installation of the latest version of Thirtyseven4 Endpoint Security is complete, open the previous version of Thirtyseven4 Endpoint Security and follow these steps:

- i. Go to Admin **Settings** > **Server** > **Redirection**.
- ii. In **Server Name/IP** text box, type the server name or IP address of the latest version of Thirtyseven4 Endpoint Security.

If the higher version of TSEPS is installed on DHCP based IP, we recommend that you use server name.

- iii. In **Port** text box, type the port number of the latest version of Endpoint Security.
- iv. Click **Apply**.

This will send a notification about the latest version of Thirtyseven4 Endpoint Security to all Thirtyseven4 endpoints and they would be redirected to the latest version.

4. The latest version of Thirtyseven4 Endpoint Security checks if there are any previous versions of endpoints in the network. If detected, Thirtyseven4 Endpoint Security will automatically uninstall the previous version of endpoints and install the latest version.
5. After all the endpoints are upgraded, you can uninstall the previous version of Thirtyseven4 Endpoint Security server.

Before uninstallation, note down the Product Key of your Thirtyseven4 Endpoint Security that will be required for re-activation of the latest version of Thirtyseven4 Endpoint Security.

6. After uninstallation of the previous version of Thirtyseven4 Endpoint Security, re-activate the latest version of Thirtyseven4 Endpoint Security with your existing product key.



You can upgrade all the endpoints with the latest version within 30/60/90 days. The Default is set to 60 days. These settings can be configured from Admin Settings > Server > General > Multi server migration period, on higher version TSEPS server when in multi-server mode.

Post Installation Tasks

Thirtyseven4 Endpoint Security must be registered immediately after installation to activate the copy, otherwise endpoint deployment will not start.

Registration

Thirtyseven4 Endpoint Security is simple to register.

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 7.2 > Activate Thirtyseven4 EPS Console**.
2. On the Registration Wizard, type the product key and then click **Next**.
3. Type relevant information in the Purchased from, Register for and Name text boxes.
4. Click **Next**.
5. Type your personal details such as organization's email address, administrator email address, contact number, and location details.
6. 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.

7. To confirm, click **Next**.

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

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

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



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

Internet Settings

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

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

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

The Configure Proxy Settings screen appears.

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

The proxy settings details are activated.

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

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

You can also set authentication rule if you use Firewall or proxy server. For this, type the User Name and Password in the Authentication section.

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

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

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

Reactivation

This section includes the following:

Reactivating Thirtyseven4 Endpoint Security

Reactivation is a facility that ensures that you use the product for the full period until your license expires. Reactivation is very helpful in case you clean your endpoint where all software products are removed, or you want to install Thirtyseven4 Endpoint Security on another endpoints. In such cases, you need to reinstall and re-activate Thirtyseven4 Endpoint Security on your system.

The reactivation process is similar to the activation process, with the exception that you need not type the complete personal details again. On submitting the product key, the details are displayed. Complete the process by verifying the details.

Note: If your license has expired and you try to reactivate it, a message about it is displayed.

Configuring Update Manager

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

Accessing Update Manager

To access Update Manager, select **Start > Programs > Thirtyseven4 EPS Console 7.2 > Update Manager**.

Features of Update Manager

Update Manager includes the following features:

- Status
- Configuration
- Connection Settings
- Reports

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. Select **Start > Programs > Thirtyseven4 EPS Console 7.2 > Update Manager**.
2. Click **Configuration**.
3. Type the Super Administrator Password and then click **OK**.
4. If you want to take the updates automatically, select **Enable Automatic Updates**.
This feature is enabled by default. We recommends that you do not disable this feature.
5. Select the update mode from the following:
 - **Internet Center:** Helps you download the updates to your system from the default Internet Center.
 - **Specified URL:** Helps you take the files for updates from a different endpoint using the updates downloaded by the connected system.
 - In **Server** text box, type the URL.
 - In **Port** text box, type the port number.

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

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

- **Specified path:** Helps you pick the updates from a specified folder of local system without an internet connection, you can specify the path of the local folder from where the updates are to be copied.

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.

- i. Select the **Pick from specified Path** option.

- ii. Type or browse the path to the folder where the updates have been copied in the local computer.
6. Select the **Download Thirtyseven4 Endpoint Security Service Pack** check box. This feature is enabled, by default.
7. Select the **Restrict download speed (kbps)** check box if you want to restrict the download speed. Enter the speed in the text box.
8. Verify the path mentioned in **Download updates to** box. All the Thirtyseven4 Endpoints Security products will take the updates from this centralized location.
9. Select the following check boxes:
 - **Always take backup before downloading new update:** Helps you take the backup of the existing updates before new updates are downloaded. These backups are used in case a rollback to previous update is required. This feature is enabled, by default.
 - **Delete report after:** Helps you delete the reports as per the time interval specified by you in the drop-down box. This feature is enabled, by default. The preset value of time interval in the drop-down box is 10 days.
10. To prevent unauthorized access to the Thirtyseven4 Endpoint Security settings, you should enable password protection. Select the **Enable password protection** check box. Type password and click **Ok**.
11. To save your changes, click **Apply**.

If you want to restore the default settings, click the **Default button**.

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

- Update Now
- Rollback

Fields	Definitions
Update Now	Helps you download the updates of Thirtyseven4 Endpoint Security.
Rollback	<p>Helps you take the Update Manager back to the previous update state. This feature will work only if the Always take backup before downloading new update option is selected in the Configuration section of Update Manager. The steps for performing Rollback are as follows:</p> <ul style="list-style-type: none"> • Click the Rollback button. <i>The Thirtyseven4 product for the Endpoint Security is displayed.</i> • After confirming the products to be rolled back, click the Rollback button on the displayed screen or click Close to exit the dialog box.

Schedule Scan in Update Manager

With Schedule Scan, you can define the scheduled scans for the Update Manager at certain frequency.

To configure Update Manager Schedule Scan, follow these steps:

1. Select **Start > Programs > Thirtyseven4 EPS Console 7.2 > Update Manager**.

2. Click **Configuration**.
3. Type the Super Administrator Password and then click **OK**.
4. Click **Settings**.

The Update Manager Scheduler dialog appears.

5. Select the **Custom** option and configure the following options:
 - i. In **Frequency**, select either the Daily or Weekly option.
If you select Weekly option, select the weekday from the list.
 - ii. In **Start At**, set time in hours and minutes.
 - iii. If you want to repeat scanning of the Update Manger, select the Repeat Update check box and set the frequency in days to repeat the scan.
6. Click **Apply**.

Connection Settings

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

To access Connection Settings, follow these steps:

1. Select **Start > Programs > Thirtyseven4 EPS Console 7.2 > 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 the **Connection Type** list, select **HTTP**.
2. Select **Enable Proxy**.
3. In Server, type the IP address of the proxy server or domain name (Example: proxy.yourcompany.com).
4. In Port, type the port number of the proxy server (Example: 80).
5. If required, type your logon credentials in User Name and Password fields to Authenticate in case of firewall or proxy server section.
6. To save the changes, click **Apply**.

If you want to restore the default settings, click the **Default** button.

Reports

The Reports section includes a log of updates or rollback activity. It provides the details such as Date, Time, and Status of the updates or rollback activity.

To access Reports, follow these steps:

1. Select **Start > Programs > Thirtyseven4 EPS Console 7.2 > Update Manager**.

2. Click **Reports**.

You can perform the following actions on reports:

Fields	Description
View	Select a report and click View to get the complete details of the downloaded update or rollback.
Delete	Select a report and click Delete to delete the report.
Delete All	Click Delete All 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 print copy of the report.
Close	Helps you exit from the report window.

Configuring ports on the Azure or AWS Cloud machine

You should configure the ports to establish communication between the TSEPS server and the clients. Allow the ports of TSEPS server, Database, Patch Server, and Update Manager in the cloud machine where TSEPS will be deployed.

Allow the following ports from the Azure or AWS machines:

- TSEPS Console - 9105
- CGI - 6799
- Download - 8095
- Communication - 5051
- MySQL - 62222
- Patch Server - 6201
- Patch Server HTTP - 3698

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 7.2 > Uninstall TSEPS Console**.
2. Thirtyseven4 Endpoint Security Uninstaller will prompt for the password.
3. Type Super Administrator Password.
4. Click **Next**.
5. After the uninstallation, the product key is displayed.

*Note down the product key as you might require it when you reinstall the Thirtyseven4 Endpoint Security. Select **Restart System Now** to restart the system immediately or **Restart system later** to restart the computer after sometime.*

6. To complete uninstallation of Thirtyseven4 Endpoint Security, click **Finish**.



- If you have assigned a script to install endpoint by Login Script Setup to domain servers, clear it through the Login Script Setup before proceeding with uninstallation.
- Before proceeding with uninstallation, ensure that all other running programs are closed.

Chapter 4. About Thirtyseven4 Endpoint Security Dashboard

Thirtyseven4 Endpoint security has a web-based graphical console that displays the current status of the health of endpoints and highlights critical security situations that need immediate attention.

This section explains how to navigate the Web console.

Log on the Thirtyseven4 Endpoint Security Web console

To log on the Web console, follow these steps:

1. Select **Start > Programs > Thirtyseven4 EPS Console 7.2**

Alternatively, you can do the following to log on:

Open the browser on a computer in your network, and do one of the following:

- In the address bar, type the TSEPS server name or IP address in the following URL format:
 - For XP: `http://{Thirtyseven4_Endpoint_Security_Server_name or IP address}/qhscan72`
 - For other OS: `http://{Thirtyseven4_Endpoint_Security_Server_name or IP address}:{port number}`
- If your system uses SSL, type the TSEPS server name or IP address in the following URL format in the address bar:
 - For XP: `https://{Thirtyseven4_Endpoint_Security_Server_name or IP address}/qhscan72`
 - For other OS: `https://{Thirtyseven4_Endpoint_Security_Server_name or IP address}:{port number}`

The Thirtyseven4 Endpoint Security Account Login window appears.

2. Type the user name as 'administrator' in the **User Name** text box and administrator password in the **Password** text box.
3. Click the **Login** button.

The Web console appears with a summary of the current health status of the network.

Resetting the Web console password

You can reset the web console password using any of the following methods:

- Use the 'Forgot Password' link
- Use the Password Reset tool

Resetting the Web console password with Forgot Password link

To reset the Web console password, follow these steps:

1. In the Account Login window, click Forgot Password link.
2. In the Reset Password window, enter username.
3. Click the **Send Recovery Email** button to generate temporary password. The Temporary Password will be sent to your registered email ID.
4. In the **Temporary Password** text box, enter the temporary password.
5. Click **Submit**.
6. In the new window, in the **New Password** and **Confirm Password** boxes, type the password to reset your password.
7. Click **Submit**.

You can log on the Web console with new password.



If SMTP settings are not configured, user can reset the password using the Password Reset tool.

Resetting the Web console password with Password Reset tool

To reset the Web console password with Password Reset tool, the user should have administrative privilege on the machine where TSEPS is installed.

To reset the Web console password, follow these steps:

1. Go to < installation directory>/ Admin/resetpwd.exe. <installation directory> indicates the path where Thirtyseven4 Endpoint Security has been installed.
2. Execute the file resetpwd.exe.
3. In the Console Password Reset Tool window, either enter Windows Host name\administrator user and password or you can select hostname\administrator from the drop down list.
4. Click **Next**.
5. In the new window, in the **New Password** and **Confirm Password** boxes, type the password to reset your password.
6. Click **Change Password**.

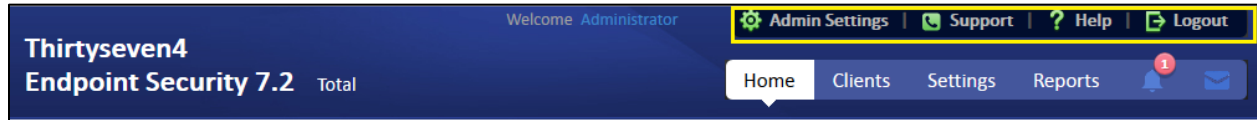
You can log on the Web console with new password.



Number of login attempts allowed are limited to 6. After 6 unsuccessful attempts, the user account will be locked for 6 hours.

Areas on the web console

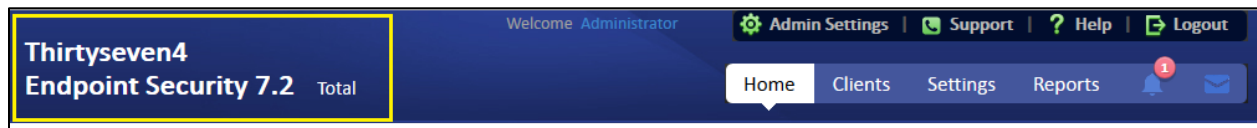
When you log on to the Thirtyseven4 Endpoint Security console, the Home page is displayed by default. The options that appear on the console are as follows:



The menu bar on the upper-right corner, highlighted in yellow, includes the following options that are common to all pages:

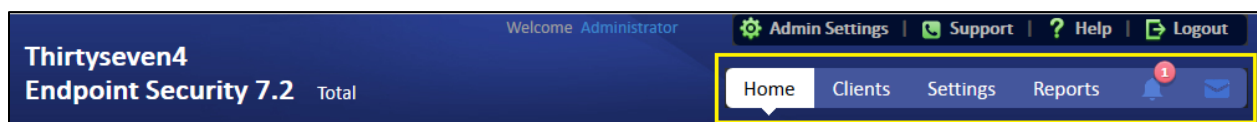
Menus	Description
Admin Settings	Helps you configure the settings related to the features such as Server and Endpoints.
Support	Helps you find out all the support options that Thirtyseven4 provides.
Help	Includes the Help file that provides information about all the features, how they work and how to configure them.
Logout	With this button, you can log out from the current session.

Product name:



The product name section includes the following:

Menu	Description
Product Name and Version	Displays the product name and its current version.

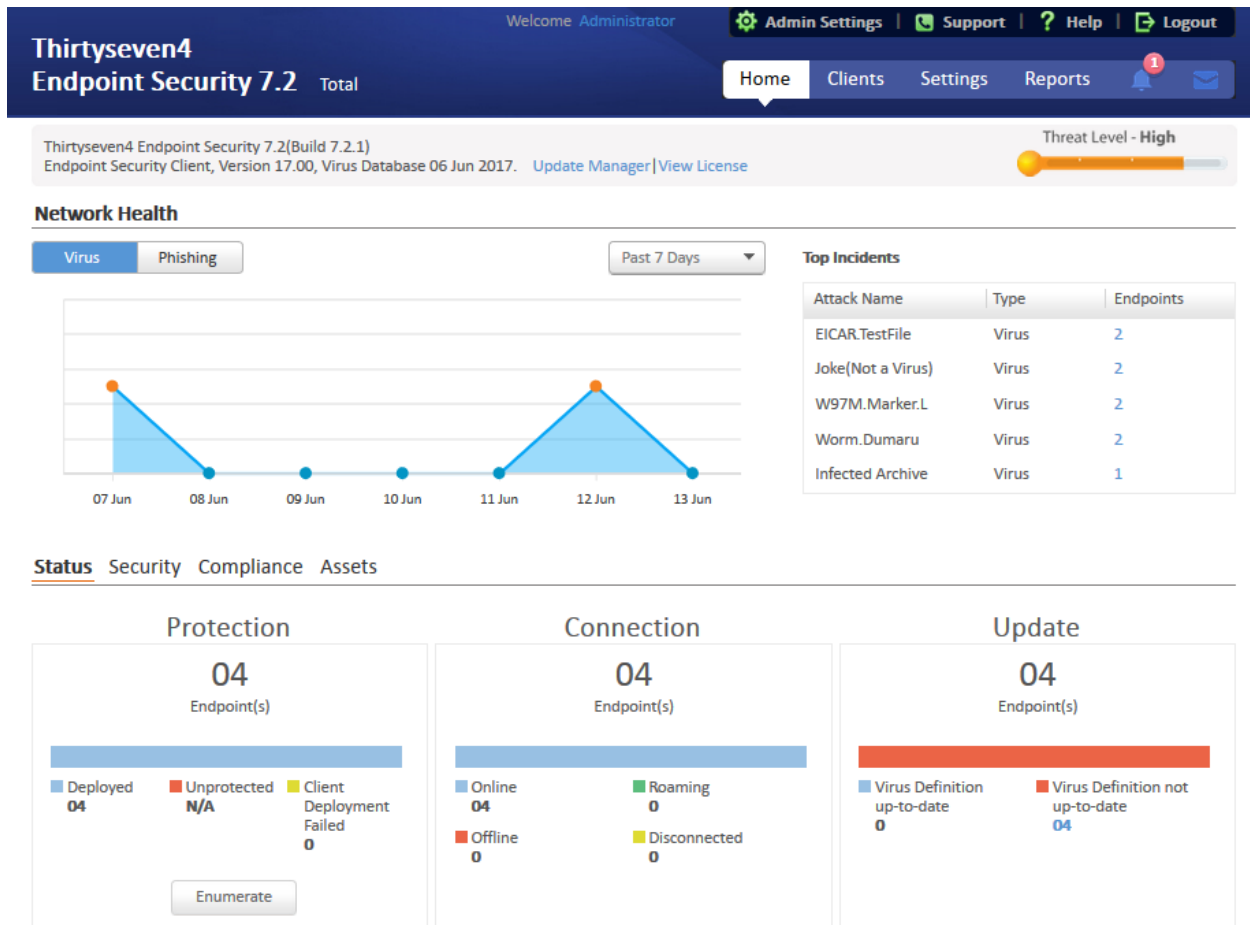


The user interface of the Web console also includes the links to the following pages:

Pages	Description
Home	Helps you visit the Home page, which is the Thirtyseven4 Endpoint Security Dashboard.
Clients	Helps you configure the settings related to Endpoint Status and Endpoint Action.
Settings	Helps you configure the settings related to Endpoint Settings and Schedule Settings.
Reports	Helps you generate reports on all the features that you need.

Alerts (Bell icon)	Displays alert messages for the following critical situations: <ul style="list-style-type: none"> Update Manager not updated License expired License limit exceeded License about to expire New service pack available
Messenger	Displays the messages related to security information, new service pack released, new TEPS version released etc.

Dashboard Area



The Dashboard area on the Home page has widgets for the following:

Overview

Feature	Description
Product version	Displays the product version along with the build number. The build number is useful for troubleshooting purposes. The TEPS service pack information is also available. The virus database date included helps in understanding if your version is updated or whether it needs updates.

Feature	Description
Update Manager	Link for running the Update Manager. For more information, See Update Manager .
View license	Displays the links for: <ul style="list-style-type: none"> Status: Displays currently held licensee information, installation number, product key, product type, validity and the maximum number of the Endpoints permitted. License order form: Displays the License order form to order new feature/license License History: Displays the license history details.
Threat Level	Displays current threat level of your network. The threat levels include: <ul style="list-style-type: none"> Normal: Indicates that 12% of the endpoints detected viral infection in last 24 hours. Elevated: Indicates that 24% of the endpoints detected viral infection in last 24 hours. High: Indicates that 36% of the endpoints detected viral infection in last 24 hours. Critical: Indicates that more than 36% of the endpoints detected viral infection in last 24 hours. Important: Thorough scanning of the entire network is recommended if the threat level alert is High or Critical.
Alert	An alert appears if the health of the network needs an immediate action. Click the More link 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

Feature	Description
Network Health	Graphical representation of the network health for the categories of Virus and Phishing. Click the respective tab to get the details of that category. It shows how secure your system is currently. This status is displayed over a 4-level grid by colored dots that are in ascending level with green at the lowest level and red at the highest level. These colored dots indicate the following: <ul style="list-style-type: none"> Green (Normal): Indicates endpoint is not infected and is secure. Yellow (Elevated): Indicates low level of endpoint infection. Orange (High): Indicates high level of endpoint infection that requires immediate action. Red (Critical): Indicates critical level of endpoint infection that requires immediate action. The right pane carries a table with Top Attacks, the type and the total number of endpoints affected.
View for drop down list	Gives a graphical representation of the network health for the selected time period. The graphs can be viewed for the following time periods: <ul style="list-style-type: none"> Past 7 Days: Displays the report of the last seven days. Today: Displays the report of the today's infection. Past 15 Days: Displays the report of the last 15 days. Past 30 Days: Displays the report of the last 30 days.

Top Attacks	Displays the top attacks on computers by Attack Name, type, and number of endpoints infected. Clicking the endpoint count opens a window with details of the actual endpoint infected.
-------------	--

Status

Feature	Description
Status Tab	Displays the information for the following categories: <ul style="list-style-type: none"> Protection Connection Update
Protection	Displays the number of endpoints deployed in the network, unprotected endpoints across your network and the endpoints on which deployment of any client has failed.
Connection	Displays the total number of connections registered to the system with the break-up for online, offline, disconnected, and roaming endpoints. It also displays information about offline, disconnected, roaming endpoints and when they were last connected to the computer.
Update	Displays the number of endpoints on which the virus definitions are not up-to-date. Click the number under the category to check information about the Endpoint name, Domain, IP address, and Virus Database date.
Enumerate	Click Enumerate to generate a list of all the unprotected endpoints connected to the network. Note: This may take some time and a link to a list of all these endpoints with their endpoint name, domain name and operating system platform name will be displayed.

Security

Feature	Description
Security Tab	Displays the protection status for the following : <ul style="list-style-type: none"> Virus protection Phishing protection Browsing Protection
Web Security	Displays the information for top 5 Web site categories, which were blocked in past 7 days in graph and a list of the top 5 Web sites, which were blocked in past 7 days in a table with URL, Type and Count columns. Note: This feature is optional and will be visible only if you have purchased the license for Web Security feature. For more information, see Web Security .
Data Loss Prevention	Displays the number of data leak attempts over the last 7 days and a list of the top users who were trying to leak the data. Note: This feature is optional and will be visible only if you have purchased the license for DLP feature. For more information, see Data Loss Prevention .
Vulnerabilities	Displays the number of affected endpoints and a comparative list of the top vulnerabilities, severity level and the total number of vulnerabilities detected. Also, displays a graphical widget for the listed data.

Patch Management	Displays the number of missing and installed patches by severity.
------------------	---

Compliance

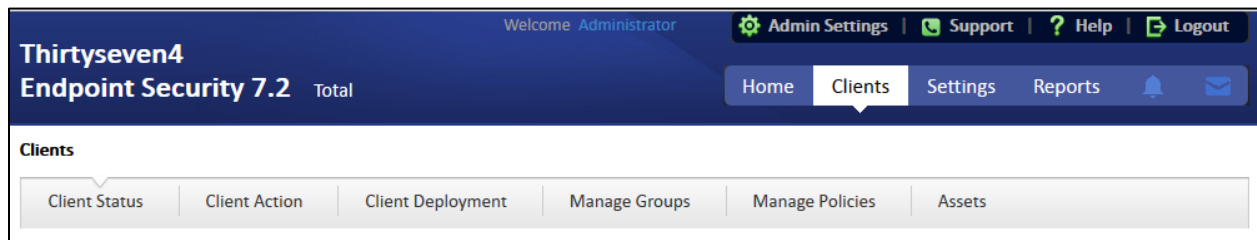
Feature	Description
Advanced Device Control	Displays the information for top device types that breached the policies in the past 7 days and a list of top 5 users who breached the policy specifying their user name, endpoint name and the count of breaches.
Application Control	Displays the information for top applications that were blocked in the past 7 days and a list of top 5 users who attempted to access the blocked applications specifying their user name, endpoint name and count.

Assets

Feature	Description
Hardware changes	Displays the number of hardware changes detected on TSEPS 7.2 endpoints only for the endpoints with Windows operating system.
Software changes	Displays the number of software changes detected on TSEPS 7.2 endpoints only for the endpoints with Windows operating system.
Platforms	<p>Displays the total number of endpoints installed on a platform.</p> <p>Click the columns in the bar graph to display extended information related to a specific category. The endpoint IP address is displayed along with the platform on which it was installed.</p> <p>Note: This feature is applicable to all endpoints for Windows, and MAC operating systems.</p>
Software Installed	<p>Displays the number of endpoints on which software have been installed. This display is also in the form of a bar graph which can be toggled to display the number of software least installed v/s the number of software most installed. Click the columns in the bar graph to display more information related to the category.</p> <p>The endpoint IP address is displayed along with the software name. This feature is applicable only for endpoints with Windows operating system.</p>

Chapter 5. Clients

The Clients page includes features that help you manage and control all the clients deployed in the network. You can verify the current status of the clients and carry out various activities. You can scan endpoint computers, update the software application, improve system performance, install and uninstall Thirtyseven4 Endpoint Security Client remotely. You can also manage endpoint groups, create and apply scanning policies etc.



The following features are available in the Clients tab as shown in the above screen:

- Client Status
- Client Action
- Client Deployment
- Manage Groups
- Manage Policies
- Assets

Client Status tab

Client Status tab gives the current status of all the endpoints in the network. The status includes information such as the endpoint name, group name, domain name, IP and MAC addresses. The tab also shows protection status, installation status, product version, virus database date, last scan date, protection policies among others, and the enabled security features.

To view the Client Status, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Client Status**.
2. Under TSEPS Console, select a group name.
3. In the right pane, all the endpoints of a relevant group are displayed.
4. Select an endpoint and click **View Status**.

The status of the selected endpoint appears.

It also includes a View Installer Log link that helps you view if Thirtyseven4 is not installed on any Client endpoints. Click the View Installer Log link to view the reason why a client failed to deploy.

You can select multiple endpoints at a time to remove offline clients.

You can either export the status or take a print if required.

Terms	Definition
Show endpoints within subgroup	Helps you view endpoints 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 endpoint name.
CSV	Helps you save the report in csv format.

Client Action tab

Using the features on the Client Action tab you can, scan endpoints remotely, update virus definitions, and improve performance of the endpoints. You can also verify the compliance to security policies, for e.g. identifying unauthorized applications installed on any of the endpoints in the network.

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

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	✓	✓
Data-At-Rest Scan	✓	✓
Temporary Device Access	✓	✓
Tuneup	✓	X
Application Control Scan	✓	X
Vulnerability Scan	✓	X
Patch Scan	✓	X
Patch Install	✓	X

Scan

This feature allows remote scanning of any endpoint in the network. You can initiate a manual scan with preconfigured policies. This feature reduces the additional task of personally overseeing each target endpoint.

To initiate scanning, follow these steps:

1. Log on to the 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 the endpoints belonging to that group.

3. Under **TEPS Console**, select a group.

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

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

The selected endpoints are scanned for compliance.

You can stop scanning by clicking Notify Stop Scan at any time you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps you display the endpoints that are in a subgroup.
Scan Settings	Helps you customize scan settings.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Refresh	Updates the status of the sent notifications.
Scan All	Helps you scan all the endpoints with a single click of the button.

Scan Settings

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

To configure Scan settings, follow these steps:

1. Log on to the 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, do the following:

- i. In How to Scan section, select either Quick Scan or Full System Scan.

Quick Scan includes scanning of the drive where operating system is installed and Full System 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. When the Advanced scan mode check box is selected, all the related attributes get enabled. You can carry out the following actions:
 - a. From the Select the items to scan options, select the files, file types (executable files, packed files, archive files), and the mailboxes that you want to scan.
 - b. In Archive Scan Level, set the scan level.

You can set the level for scanning in an archive file. The default scan level is 2. Increasing the default scan level may affect the scanning speed.
 - c. To remove an infected file from your system, follow these steps in the Select action tab:
 - If an infected file is found in an archived folder on your system, select whether you want to delete, quarantine, or skip the file.
 - If an infected file is found in your active folder/drives on your system, select whether you want to repair, delete, or skip the file.
- iv. Under Antimalware Scan Settings, select **Perform Antimalware** scan if required.
- v. In Select action to be performed when malware found, select an action from the following:
 - Clean
 - Skip

The action selected here will be taken automatically.

- vi. Under Boot Time Scan Settings, select **Perform Boot Time Scan**.

The Select Boot Time Scan Mode option is activated.
- vii. Select one of the following scan options:
 - Quick Scan
 - Full System Scan

The setting for Boot Time Scan is applied only once and is not saved.

- viii. After configuring the scan setting, click **Apply**.

The new setting is applied.



- Scan packed files, Scan mailboxes, Antimalware Scan Settings, and Boot Time Scan Settings are available only in the clients with Windows operating systems.
- Notification for Scan from TSEPS web console will not be sent if the user is not logged on to the Mac system.

Update

Using this feature, you can update the client applications on any endpoint in the network remotely. Thirtyseven4 releases updates regularly to fix technical issues and provide protection against new threats. Hence, it is recommended that you update the virus definitions of your software protection regularly.

To take the update, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and select **Clients > Client Action**.
2. Click **Update**.

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

3. Under TSEPS Console, select a group.

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

4. Select an endpoint and then click **Notify Update Now**.

The selected endpoints are updated with the latest virus definitions.

Terms	Definition
Select endpoints with out-of-date Thirtyseven4	Helps you update endpoints with outdated virus definitions.
Show endpoints within subgroup	Helps you display endpoints that are in a subgroup.
Notify Update Now	Helps you notify endpoints to update Thirtyseven4.
Refresh	Updates the status of sent notifications.
Update All	Helps you update all the endpoints with a single click of the button.



Notification for update from TSEPS Web console will not be sent if the user is not logged on to the Mac system.

Tuneup

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



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

To tune up the endpoints, follow these steps:

1. Log on to the 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 the endpoints belonging to the group.

- Under TSEPS Console, select a group for which you want to perform the tune up process.

By default it shows all the endpoints present under the TSEPS console.

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

- Select an endpoint and then click **Notify Start Tuneup**.

Tuneup notifications are sent to the selected endpoints and tune up is performed on those endpoints.

You can stop Tuneup activity by clicking Notify Stop Tuneup at any time you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps you display those endpoints that are in a subgroup.
Tuneup Settings	Helps you customize Tuneup settings.
Notify Start Tuneup	Helps you notify the clients to start Tuneup.
Notify Stop Tuneup	Helps you notify the clients to stop Tuneup.
Refresh	Updates the status of sent notifications.
Tuneup All	Helps you tune up all the endpoints with a single click of the button.

Tuneup Settings

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

To customize Tuneup settings, follow these steps:

- Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Client Action > Tuneup**.
- On the Tuneup screen, click the **Tuneup Settings** button.
- 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.

- To save your settings, click **Apply**.

Disk Cleanup: Helps you find and remove invalid and unwanted junk files from the hard disk. These files consume hard disk space and slow down the system considerably. Disk Cleanup deletes these files and provide free 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, such entries may appear due to improper uninstallation, non-existent fonts, etc. 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 increase the performance of the 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 the system performance. Defragment reduces the number of fragments and clubs all the fragments into one contiguous chunk to improve system performance.

Application Control Scan

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



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

To scan endpoints for compliance control, follow these steps:

1. Log on to the 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 the endpoints belonging to the group.

3. Under TSEPS Console, select a group.

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

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

The selected endpoints are scanned for compliance.

You can stop scanning by clicking Notify Stop Scan at any time you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps display the endpoints that are in a subgroup.
Scan Settings	Helps you customize the scan settings for application control.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Refresh	Updates the status of the sent notifications.
Scan All	Helps you scan all the endpoints with a single click of the button.

Scan Settings

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

1. Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Client Action > Application Control Scan**.
2. On the Application Control Scan screen, click the **Scan Settings** button and then select one of the following:

Unauthorized applications: Helps you initiate scanning only for the unauthorized applications, present on a client machine.

Unauthorized and authorized applications: Helps you initiate scanning for both unauthorized and authorized applications present on the 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 longer time.

3. To save your settings, click **Apply**.

Vulnerability Scan

This feature allows you to scan the known vulnerabilities in the installed applications of various vendors such as Adobe, Apple, Mozilla, Oracle etc. and the operating systems on the endpoints in your network and assess their security status. You can probe the endpoints for applications, and operating system patches for possible vulnerabilities. This is helpful to create security measures against the known vulnerabilities and secure the endpoints against data outage.

To enable Vulnerability Scan, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Client Action**.
2. Click **Vulnerability Scan**.
3. On the Vulnerability Scan page, click the **Scan Settings** button.

The Scan Settings dialog appears.

4. Under **Scan** for vulnerability against following software vendors, select one of the following options:
 - Microsoft applications and other vendor applications
 - Microsoft applications only
 - Other vendor applications only
5. To save your settings, click **Apply**.

You can stop scanning by clicking Notify Stop Scan at any time you prefer.

Terms	Definition
-------	------------

Show offline clients	Helps you view the endpoints that are not online or disconnected from the network.
Show endpoints within subgroup	Helps display the endpoints that are in a subgroup.
Scan Settings	Helps you customize the scan settings Vulnerability Scan.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Refresh	Updates the status of the sent notifications.
Scan All	Helps you scan all the endpoints with a single click of the button.

Data-At-Rest Scan

Using Data-At-Rest Scan, you can scan, and detect any confidential data present in your endpoints and removable devices. You can scan the desired location such as drive, folder, or removable devices on the endpoints and detect the confidential or sensitive information present. You can view the information related to the detected confidential data such as the file path, threat type, and matched text.

To perform Data-At-Rest scan, you must enable DLP on the endpoints. To enable DLP on the endpoints, see [Enabling DLP feature](#).

Scan Settings

To enable Data-At-Rest Scan, follow these steps:

1. Log on to the Thirtyseven 4 Endpoint Security web console.
2. Select **Clients > Client Action**.
3. Click **Data-At-Rest Scan**.
4. Enter the endpoint name or IP address that you want to scan or select from the default list.

You can also select an endpoint from a particular group.

You may also select the required check box provided at the end of the page if you want to select an offline client or endpoint within a subgroup or both.

5. Click the Scan Settings button and select one of the following:
 - **Quick Scan:** Select this option to scan the drive on which your operating system is installed.
 - **Full System:** Select this option to scan all the drives.
 - **Scan Specific Folder(s):** Select this option to scan a particular folder(s).
 - i. Click **Configure**.
 - ii. Enter the path of the folder that you want to scan.
You can also choose to scan the subfolders by selecting the Include Subfolder check box.
 - iii. Click **Add**.

You can also remove a path from the list by clicking Remove.

iv. Click **Apply**.

6. From the File Types list, select the file format that you want to search for the data.
7. Select either Confidential Data or User Defined Dictionaries or both for the type of data that you want to scan.
8. Click **Apply**.

Clicking Cancel, closes the dialog box and clicking Default, clears all the selections.



- Data-At-Rest Scan feature is not available on Windows 2000 operating system.
- Email Notifications are not supported for Data-At-Rest Scan feature.
- Data-At-Rest Scan feature will be available only if DLP feature pack is enabled for that TSEPS server.

You can stop scanning by clicking Notify Stop Scan at any time you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or disconnected from the network.
Show endpoints within subgroup	Helps display the endpoints that are in a subgroup.
Scan Settings	Helps you customize the scan settings for application control.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Refresh	Updates the status of the sent notifications.
Scan All	Helps you scan all the endpoints with a single click of the button.

Exclusion

You may exclude or include a path for scanning.

- To exclude, enter the path in the text box and click **Add**.
- To include, select the path in the text box and click **Delete**.

Patch Scan

This feature allows you to scan the missing patches in the network.

To enable Patch Scan, follow these steps:

1. Log on to the Thirtyseven 4 Endpoint Security Web console.
2. Go to **Clients > Client Action > Patch Scan**.
3. Click the **Scan Settings** button and select one of the following options:
 - **Online (Recommended)**
The client accesses latest data from the patch server during missing patch scan.

- Offline

The client accesses data from the local system during missing patch scan.

4. Click **Apply**.

5. Enter the endpoint name or IP address that you want to scan or select from the default list.

You can also select an endpoint from a particular group.

You may also select the required check box provided at the end of the page if you want to select an offline client or endpoint within a subgroup or both.

6. Select an endpoint and then click **Notify Start Scan**.

The selected endpoints are scanned for missing patches.

We recommend to select 100 endpoints at a time for patch scan to have optimal performance.

You can stop scanning by clicking **Notify Stop Scan** whenever you prefer.

Terms	Definition
Show offline clients	Helps you view the endpoints that are not online or are disconnected from the network.
Show endpoints within subgroup	Helps display the endpoints that are in a subgroup.
Scan Settings	Helps you customize the scan settings for patch scan.
Notify Start Scan	Helps you notify the clients to start scanning.
Notify Stop Scan	Helps you notify the clients to stop scanning.
Refresh	Updates the status of the sent notifications.

Patch Install

This feature allows you to install the missing patches on the selected endpoints.

To install the missing patches, follow these steps:

1. Log on to the Thirtyseven 4 Endpoint Security Web console.
2. Go to **Clients > Client Action > Patch Install**. Patch Install page appears. A list of the missing patches appears.
3. You can filter the list with the help of the four filters described in the following tables:

Severity options:

Severity	Description
Critical	Vulnerability may allow code execution without user interaction.
Important	Vulnerability may result in compromise of the confidentiality, integrity, or availability of user data. The client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability.
Moderate	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.

Low	Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.
Unspecified	Vulnerability may result in random malfunctions.

Category options:

Category	Description
Security Updates	A widely released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated by their severity. The severity rating is indicated in the Microsoft security bulletin as critical, important, moderate, or low.
Update Rollups	A tested, cumulative set of hotfixes, security updates, critical updates, and updates that are packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a component of a product, such as Internet Information Services (IIS).
Applications	Application (software) is a subclass of computer software that employs the capabilities of a computer directly and thoroughly to a task that the user wishes to perform.
Service Packs	A tested, cumulative set of all hotfixes, security updates, critical updates, and updates. Additionally, service packs may contain additional fixes for problems that are found internally since the release of the product. Service packs may also contain a limited number of customer-requested design changes or features.
Feature Packs	New product functionality that is first distributed outside the context of a product release and that is typically included in the next full product release.
Updates	Updates are code fixes for products that are provided to individual customers when those customers experience critical problems for which no feasible workaround is available.
Definition Updates	A widely released and frequent software update that contains additions to a product's definition database. Definition databases are often used to detect objects that have specific attributes, such as malicious code, phishing websites, or junk mail.
Critical Updates	A widely released fix for a specific problem that addresses a critical, non-security-related bug.
Drivers	Software that controls the input and output of a device.

Restart Required options:

Restart Required	Description
All	Display result for all the options.
Not Required	The patch does not require the system restart.
Required	The patch requires the system restart. Restart the system to take the patch effect.
May Require	The patch may require the system restart.

EULA Status options:

EULA Status	Description
All	Display result for both the options, Accepted and Not Accepted.
Accepted	End User License agreement is accepted.
Not Accepted	End User License agreement is not accepted.

You can provide endpoint name or an application name to generate the specific result. You can search the patches by entering KB ID or Bulletin ID.

To generate the result with help of filters and/or record details, click **Generate**.

4. Select the **Show patches within subgroup** check box to display the name of the patches that are in the subgroup from the list of the endpoints without actually exploring the network.
5. To change the restart setting, click **System Restart Settings** button. Restart settings are applicable only if the patch requires the system restart.
6. Select the **Allow auto-restart the system** check box to restart the system automatically. Clear the check box to restart the system manually.
7. From the missing patches list, select the patches that you want to install.
 - a. In the list, click the number in the column No. of Endpoint Affected. Endpoint(s) affected dialog appears.
 - b. Select the endpoints where you want to install the missing patch.
 - c. Click **Apply**. The list of endpoints is saved.
8. Click **Start Install**. To cancel the selection, click **Refresh**.
9. To exclude endpoints from installing patches, click the **click here** link. Exclusion for Patch Install dialog appears.
10. Select the Exclude endpoints having Server OS in an TSEPS network check box if required.
11. Select the Exclude below endpoints check box.
12. To exclude a particular endpoint, enter the endpoint name or IP and then click Add.
13. Click Apply.

To remove the exclusion, select the endpoint and then click Remove.

Temporary Device Access

This feature allows you to permit temporary access to a device on the client for a specific period. If a user wants temporary access to a device on the client, he can send a request to the Administrator for temporary access. An OTP is generated and shared. The client uses this OTP to access the device for the specific period.

To enable Temporary Device Access, follow these steps:

1. Log on to the Thirtyseven 4 Endpoint Security Web console.
2. Go to **Clients > Client Action > Temporary Device Access**.

3. On the Temporary Device Access page, select the endpoint client which requires temporary access. Only one endpoint can be selected at a time.
4. Click **Allow Temporary Access**. The Generate OTP dialog appears.
5. In the **Allow temporary access for** list, select minutes.
6. In the **Use OTP within** list, select minutes.
7. Click **Generate**. The OTP appears. When the client is online, click **Notify** and the OTP is automatically received by the client. Temporary access is allowed as per the settings effective from that minute.
8. If the client is offline or roaming, Notify is disabled. To send the OTP manually, by Email to the client, do the following:
 - a. Click **Notify By Mail**. Mail dialog appears.
 - b. In the **To** text box, enter Email ID.
 - c. Click **Send Mail**. Default mail client of the system opens and displays a mail specifying the details of the OTP.
 - d. Click **Send**.

At the client side, after successful validation of the OTP, temporary device access is enabled for the specific period.

Chapter 6. Client Deployment

The Client Deployment tab on the Clients page helps you to deploy the Thirtyseven4 Endpoint Security client.

Select one of the following methods to deploy the Endpoint Security client as applicable. A brief about each method is mentioned below.

- Through Active Directory: Sync with Active Directory groups to deploy Endpoint Security client.
- Remote Install: Install Endpoint Security client remotely.
- Notify Install: Send e-mail notification containing URL to client Installation.
- Client Packager: Create client installer for manual installation.
- Login Script: Assign login script for client installation.
- Disk Imaging: Deploy Endpoint Security clients through imaging.

The following table shows support of different operating systems related to client deployment methods:

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

Through Active Directory

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

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

Notes:

- This installation method is available only with Microsoft Windows operating system.
- To synchronize with Active Directory your console should be installed on the domain machine or should be a member of the domain.
- Synchronization cannot be done with Default group.
- Groups shown in Red Color are already synched with Active Directory.
- The user should have permissions of Domain Admins to synchronize with Active Directory.
- The default synchronization time interval is GLOBAL.

Synchronizing with Active Directory

To sync Active Directory groups, follow these steps:

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

Editing Synchronization

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

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

To edit the time interval, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and the select **Clients > Client Deployment**.

2. Click **Through Active Directory**.

A window appears with all the groups.

3. Under TSEPS 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 this feature, you can remove the synchronization of a group in the following way:

1. Log on to the Thirtyseven4 Endpoint Security Web Console and then select **Clients > Client Deployment > Through Active Directory**.

A window appears with all the groups.

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

The synchronization of the selected group is removed successfully.

Exclusion

You can exclude endpoints from installation of TSEPS client when Active Directory is synchronized. TSEPS client will be not installed on the excluded endpoint. You can exclude endpoints by Host Name, IP Address or by IP Range.

To exclude an endpoint, follow these steps:

1. Log on to the 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, type the Host Name and click Add. The workstation is added to the Excluded Workstations list.

Exclude by IP Address: If you select this option, type the IP address and click Add. The workstation is added to the Excluded Workstations list.

Exclude by IP Range: If you select this option, type the Start IP Range and End IP Range details and click **Add**. The workstations are added to the Excluded Workstations list.

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

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

Remote Install

This feature allows you to deploy the Thirtyseven4 client on all supported Windows operating systems (OS). You can also install Thirtyseven4 client on multiple endpoints at a time. Before proceeding with Remote Install, it is recommended that you go through the following requirements and changes:

Exception Rules:

On Windows Vista and later operating systems, remote installation is possible only with 'Built-in Administrator' account. To enable 'Built-in Administrator' account on endpoints running Windows Vista (or later), follow these steps:

- i. Open Command Prompt in administrative mode.
- ii. Type 'net user administrator /active: yes' and press Enter.
- iii. 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:

- i. Open My Computer.
- ii. Go to Tools > Folder.
- iii. Click the View tab.
- iv. Clear the option Use simple file sharing.
- v. 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, such as 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 the computer which are under Domain Controller, specify the user name in 'DOMAINNAME\User Name' format where DOMAINNAME is the name of the Domain Controller and User Name is the name of the Domain Administrator.

For Remote Install, follow these steps:

1. Log on to the 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 one of the following ways:

Remote Installation by computers

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

Any endpoint in your network can be searched without enumerating the network.

For adding an endpoint you are required to provide the user credentials of the target endpoint, having administrator rights.

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

Repeat these steps for all the endpoints that you have selected. .

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

In case, if you forget or provide an incorrect user credentials of an endpoint, you can click the Skip button and move to the next endpoint and provide its user credentials.

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 endpoints 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 endpoint.

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

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

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

The Add User dialog appears.

5. 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.

6. On the User Accounts list, click **Finish**.

All the endpoints are added to the Endpoints selected to protect the list.

7. Click **Install**.

The installation status of the Thirtyseven4 client agents can be viewed through View Installation Status link.



- The Remote Install feature is available only in the clients with Windows operating systems.
- Remote Install is not supported through roaming service.

Viewing installation status

When deploying the clients with help of remote installation process, you can keep track of client installation with the help of View Installation Status link. You can get more information about installation from Results column. At any instance, you can visit Remote Installation Status page and refresh the page to get latest installation status of multiple endpoints.

This page also provides an option to stop the installation. The installation can be stopped for those endpoints, on which installation has not yet started and is in pending state. You cannot stop the installation which is in progress state.

To view installation status, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Clients > Client Deployment > Remote Install**.

The Remote Install page appears.

3. Click **View Installation Status** link.

Remote Installation Status page appears.

The page shows following columns:

- Endpoint Name: Shows names of the endpoints.
- Domain: Shows domain names.
- Date/Time: Shows the installation status date and time.
- Result: Shows installation status. If any installation fails, its reason is also displayed.
- The page also shows different buttons as follows:
 - Refresh: On refresh, the latest result of client installation on multiple endpoints is displayed.
 - Stop Installation: Stops the pending installation, which is not actually started. You cannot stop the installation which is in progress.

- Clear: This option helps to clear the installation information from the Result column about successful, failed, and stopped client installation.
- Close: It closes the installation status page.

Notify Install

This facility allows you to send email notification to the endpoints in the network to install the Thirtyseven4 Endpoint Security client. The message can be typed and saved for future notifications. This can be edited whenever required.

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

1. Log on to the 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 semicolon (;) 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 email using the email program.

Users have to click the link provided in the email that will redirect to Thirtyseven4 client installation Web page.

4. Click the **Download** button and download the client installation utility. Execute the cainstlr.exe file.

After Thirtyseven4 client installation is finished, the Thirtyseven4 Antivirus installation will be initiated by the Thirtyseven4 client.



- The Notify Install feature is available only in the clients with Microsoft Windows and Mac operating systems.
- To download the Notify Install utility, few Internet Explorer settings should be configured as follows:
 - Internet Explorer Settings for Windows Server 2008:
 - With the help of Server Manager, configure IE ESC and turn off for both Administrators & Users.
 - From Internet Explorer, go to Tools > Internet Options > Advanced tab. Clear the following check box, Check for signature on downloaded programs.
 - Internet Explorer Settings for Windows Server 2003:
 - From Internet Explorer, go to Tools > Internet Options > Advanced tab. Clear the following check boxes, Do not save encrypted pages to disk, and Empty Temporary Internet Files folder when browser is closed.
 - Other Security Settings for Internet Explorer:

Other Internet options which are to be enabled are;

 - Enable File download feature in Custom level security settings.
 - Enable advanced security settings by selecting Allow software to run or install even if signature is invalid check box.

- Once Notify client utility is downloaded on your system then you can revert the settings done in Internet Explorer to previous state.

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 the Client Packager tool. The Client Packager can also be created for the Clients outside the organizational network using the Minimal option.

In Thirtyseven4 Endpoint Security 7.2, Client Packager can be created with or without the Thirtyseven4 installer and also with MSI-based Client Packager. The Client agent installer including Thirtyseven4 installer is helpful in situations where there are network bandwidth limitations to download the Thirtyseven4 installer from the Endpoint Security server. In such cases, you can create the Client agent installer including the Thirtyseven4 installer and burn into a CD/DVD or copy it to a USB removable disk for deployment on endpoints. But, the Client Packager with the installer cannot be distributed through email.

When you receive the package, double-click the setup program to start the installation. The Thirtyseven4 clients installed through Client Packager starts communicating with the Thirtyseven4 Endpoint Security server.



The Thirtyseven4 Clients installed through Client Packager out of organizational network, communicates with Thirtyseven4 Endpoint Security server by using roaming service.

Creating Windows Thirtyseven4 Client Packager

To create a Windows Thirtyseven4 Client package, follow these steps:

1. Go to **Start > Programs > Thirtyseven4 EPS Console 7.2 > Client Packager**.
2. In Client Agent Package list, select **Custom**.

*If **Minimal** is selected then the Validity period check box is enabled, but other options on the page gets disabled. The validity period check box helps you to provide a stipulated number of days to use the installer. After the validity period, the installer expires.*

*The **Minimal** option is selected to send the Client Packager outside the organizational network through email. For more details see, [Sending a minimal Client Packager](#). The Client Packager created with installer cannot be sent through email because of its huge size.*

3. In OS platform list, select Windows.
4. Select the setup type from Setup type list as per requirement.

EXE/32-bit for 32-bit Client Packager EXE/64-bit for 64-bit Client Packager	Select EXE/32-bit or EXE/64-bit options to create the packager as an executable file.
MSI/32-bit for 32-bit Client Packager	Select MSI/32-bit or MSI/64-bit options to create the packager as a Microsoft installer package. These packages are useful in deploying the Thirtyseven4 clients through the following:

MSI/64-bit for 64-bit Client Packager	<ul style="list-style-type: none"> • Active Directory group policies • Microsoft SMS server
---------------------------------------	---

5. Specify if you want to include antivirus setup in Client Packager by selecting Yes or No.

Select Yes, if you want to include the antivirus setup in Client Packager. But you cannot distribute this packager through email.

Select No, if you do not want to include the antivirus setup in Client Packager. This packager can be distributed through email.

6. A Default group is allocated to the Client Packager from the TSEPS Console groups list.

The selected group gets assigned to the Client Packager and the installed client through that Client Packager will move to the selected group of TSEPS Console.

7. Click Browse to specify the folder path where you want to save Thirtyseven4 Client Packager.

8. Select the **Select this check box to specify public IP address/Hostname of TSEPS server for deployment of clients at remote locations** check box.

Type the Public IP address or Hostname of the TSEPS server.

In case of Public installation, the check box and public IP address/Hostname fields does not appear.

9. Click **Create**.

10. Specify if you want to create a password protected Client Packager by selecting Yes or No.

If you select Yes, password dialog appears. Do the following:

- Type the password and then click OK.
- Use a password that has at least 6 characters and maximum 18 characters. While creating the password use combination of number, uppercase letter, lowercase letter and special symbol.
- In the Confirmation Password box, enter the password.
- Click OK. A password protected Client Packager is created.
- Provide the password while extracting the client packager.

If you select No, Client Packager without password protection is created.

Password Protection is applicable only for EXE setup types for the Windows client.

Creating Mac Thirtyseven4 Client Packager

To create a Mac Thirtyseven4 Client package, follow these steps:

Open Client Packager on TSEPS server following the listed path:

- Go to **Start > Programs > Thirtyseven4 EPS Console 7.2 > Client Packager**
- In the Client Agent Package list, select **Custom**.

3. In the OS platform list, select Mac.
4. A Default group is allocated to the Client Packager from the TSEPS Console groups list.
The selected group gets assigned to the Client Packager and the installed client through that Client Packager will move to the selected group of TSEPS Console.

5. Specify whether you want to include antivirus setup in Client Packager by selecting Yes or No from Antivirus setup included list.

Select Yes if you want to include the antivirus setup in Client Packager. However, you cannot distribute this installer through email.

Select No if you do not want to include the antivirus setup in Client Packager. This installer can be distributed through email.

6. Download the Mac Client build from the following URL:
<http://updates.thirtyseven4.com/builds/2016/eps7.2/mclsetp.zip>

After downloading, copy it and extract build to,

“Thirtyseven4\Endpoint Security 7.2\Admin\Web\build\”

7. Click Create.

If you select Yes to include antivirus in the client packager, a MCCLAGAV.TAR file is created in the acmac folder.

If you select No to create the client packager without antivirus, a MCCLAGNT.TAR file is created in the acmac folder.

8. On the Mac endpoint you need to copy and extract any of the above created TAR file and Run the MCLAGNT.DMG file from the extracted folder to install Mac Thirtyseven4 Client. When the administrator downloads MCCLAGNT.TAR from the link provided in the e-mail for ‘Notify Install’, the setup will be downloaded from the ACMAC folder of TSEPS server.



For roaming endpoints with MAC OS, only Custom client packager can be used for installing TSEPS client.

Sending the package through email

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

Sending a minimal Client Packager

To send Client Packager from the server through an email for out of network usage, follow these steps:

1. Go to **Start > Programs > Thirtyseven4 EPS Console > Client Packager**.
2. In the Client Agent Package list, select **Minimal**.
Few options on the page become disabled.
3. Default group is selected by default under which the client will be managed after installation.

4. Click **Browse** to specify the folder path where you have saved the Thirtyseven4 Client Packager.

5. 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.

6. 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.*

7. Click **Send**.

Sending a custom Client Packager

To send Client Packager from the server through an email for internal network, follow these steps:

1. Go to **Start > Programs > Thirtyseven4 EPS Console > Client Packager**.
2. In the Client Agent Package list, select **Custom**.
3. Default group is selected by default under which the client will be managed after installation.
4. Click **Browse** to specify the folder path where you have saved the Thirtyseven4 Client Packager.

5. 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.

6. 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.*

7. Click **Send**.



Send mail button will remain disabled for Mac Client Packager and Client Agent installer including Thirtyseven4 installer option.

Login Script

This section includes the following.

Installing Login Script

This feature allows you to assign a login script to the users so that they can deploy Thirtyseven4 Client on remote systems when they log on to the selected domain. You can assign a script called QHEPS.BAT to the selected users in the domain. This script will install Thirtyseven4 Endpoint Protection on the system when the user logs on to the concerned domain.



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

Opening Login Script Setup

To open the Login Script Setup, follow these steps:

1. Select **Start > Programs > Thirtyseven4 EPS Console 7.2**.
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. Open Login Script Setup; follow the steps mentioned in the Opening Login Script Setup section.
2. In the new screen, double-click the **Domain**.
3. Click the **Domain Name**.
4. 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**.
5. Select Overwrite existing Login Script if you want to overwrite the existing assigned login script of the selected users.
6. 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.

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

Installing Thirtyseven4 Endpoint Security on Mac Operating Endpoints

Before continuing, create a Mac Client Packager (Refer [Creating Mac Thirtyseven4 Client Packager](#))

After the Mac Client Packager has been created, the administrator can install TSEPS client using Notify Install method.

Notify Install allows you to send email notification to the endpoints in the network to install the Thirtyseven4 Endpoint Security client.

To notify clients to install the Thirtyseven4 client, see [Notify Install](#).

A Notify Install message containing a link for the installer file is sent from the administrator before installing Thirtyseven4 Endpoint Security.

To install Thirtyseven4 Endpoint Security, follow these steps:

1. To install TSEPS Client on a Mac system, type the link in the browser (sent to you in the email).

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 the Download Mac Client link.

A file MCCLAGNT.TAR 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 (MCLAGNT.DMG).

Run the installer to start the Thirtyseven4 Endpoint Security installation.

Thirtyseven4 Endpoint Security is installed successfully.



Installation of Standalone Thirtyseven4 Total Security for Mac build will proceed even if TSEPS client is installed.

Remote Installation of Thirtyseven4 Endpoint Security on Mac System

You can install Thirtyseven4 Mac Client Agent in any of the following ways.

- Installing using Apple Remote Desktop or Casper
- Connecting remotely using Secure Shell
- Using Terminal (for Mac OS)
- Using PuTTY (for Windows OS)

Remote installation using Apple Remote Desktop or Casper

Apple Remote Desktop (ARD) helps you to connect to the Mac client computers remotely in the network, send software to them, install software on them, help other end users in real time, and perform various tasks.

Prerequisites

Before you install Thirtyseven4 Mac Client Agent, ensure the following requirements.

- The administrator computer with ARD or Casper installed must have Mac OS 10.6 or later / OS X server.
- Mac Thirtyseven4 Client installer must be created on Thirtyseven4 Endpoint Security (SEPS) server. To know about how to create client installer, see [Creating the Mac Thirtyseven4 Client installer](#).
- Administrator must have an account on the Mac client computers with admin privileges.
- Enable Remote Management on the Mac client computers.
- Your administrator computer must have Packages installed on it. Packages is a Mac OS application that helps you to create bundle for your payload and installation. To download Packages, visit <http://s.sudre.free.fr/Software/Packages/about.html>.

Creating Client Agent package

To create Client Agent package, follow these steps:

1. On the Thirtyseven4 Endpoint Security server, browse to the folder “<installation directory>\Thirtyseven4\Endpoint Security 7.2\Admin\web\build”.
- <installation directory> indicates the path where Thirtyseven4 Endpoint Security has been installed.*
2. Copy the folder acmac to the administrator Mac computer.
3. Open Terminal.app on the administrator Mac computer and go to the acmac folder.
4. Enter the following commands:

```
cd ./Remote_Installation/PKG
sudo sh ./ClientAgentInstaller/CreatePackage.sh
```



Administrator rights are required for executing this command.

When the package creation completes successfully, ClientAgentInstaller.pkg file is created in the ./Remote_Installation/PKG/ClientAgentInstaller/ folder.

Installing Client Agent using Apple Remote Desktop or Casper

This procedure has been provided to help you install Client Agent on the remote Mac client computers using ARD or Casper. For more details, you may consult the documentation of the respective software applications.

Deploying Thirtyseven4 Mac Client Using Apple Remote Desktop

In addition to the Prerequisites described in the preceding section, follow this prerequisite.

Prerequisite

Before deploying Thirtyseven4 Mac Client, ensure that you get Apple Remote Desktop (ARD) tool installed on your administrator computer. To download ARD, visit <https://www.apple.com/in/remotedesktop/>.

To deploy Thirtyseven4 Mac Client using Apple Remote Desktop, follow these steps:

1. Open Apple Remote Desktop.

2. Select the Mac client computers from the list of all available computers and then click Install to add the package.
3. Click the plus (+) sign to locate and add ClientAgentInstaller.pkg and then click Install to begin deployment.

Deploying Thirtyseven4 Mac Client Using Casper

In addition to the Prerequisites described in the preceding section, follow this prerequisite.

Prerequisite

Before deploying Thirtyseven4 Mac Client, ensure that you get Casper tool installed on your administrator computer. Casper helps to install software and run scripts remotely on the client computers. To download Casper, visit <http://www.jamfsoftware.com/products/casper-suite/>.

To deploy Thirtyseven4 Mac Client using Casper, follow these steps:

1. Log on to Casper Admin.
2. Drag **ClientAgentInstaller.pkg** to the window and then select **File > Save**.
3. Log on to Casper Remote.
4. In the Computers tab, select the Mac client computers from the list of available computers.
5. In the Packages tab, select ClientAgentInstaller.pkg.
6. Click Go.

Connecting remotely using Secure Shell

Secure Shell (SSH) is a network protocol that is used to connect to the remote Mac client computers over secure data communication through command line to manage client computers.

Using Terminal (for Mac OS)

The administrator computer having either Mac OS can install Client Agent using this method.

Prerequisites

Before you install Thirtyseven4 Mac Client Agent, ensure the following requirements.

- Administrator must have an account on the Mac client computers with admin privileges.
- Enable Remote Login and either allow access for all users, or only for specific users, such as Administrators. You can find this setting on the Mac computer under System Preferences > Sharing > Remote Login.
- Ensure that the firewall does not block the port that Secure Shell (SSH) uses, which is by default TCP port 22. This port allows the required communication for remote login.
- If you use the Mac firewall, disable stealth mode. With stealth mode enabled, the remote push installation cannot discover the client through Search Network.
- To disable stealth mode on the Mac computers, see the following Apple knowledge base article that applies to your version of the Mac operating system.
 - For 10.8, OS X Mountain Lion: see [Prevent others from discovering your computer](#).

- For 10.9, OS X Mavericks: see [Prevent others from discovering your Mac](#).
- For 10.10, OS X Yosemite: see [Prevent others from discovering your Mac](#).
- For 10.11, OS X El Capitan: see [Prevent others from discovering your Mac](#)
- For 10.12, macOS Sierra: see [Prevent others from discovering your Mac](#)
- Mac Thirtyseven4 Client installer must be created on the Thirtyseven4 Endpoint Security server. To know about how to create client installer, see [Creating the Mac Thirtyseven4 Client installer](#).

Installing Thirtyseven4 Mac Client Agent

To install Thirtyseven4 Mac Client Agent using Terminal, follow these steps:

1. On the Thirtyseven4 Endpoint Security server, browse to the folder “<installation directory>\Thirtyseven4\Endpoint Security 7.2\Admin\web\build”.
- <installation directory> indicates the path where Thirtyseven4 Endpoint Security has been installed.*
2. Copy the folder acmac to the administrator Mac computer.
3. Open Terminal on the Mac administrator computer and go to the acmac/Remote_Installation folder.
4. Enter the following command

```
sh ./Scripts/copy.sh <username> <ip_address>
```

Parameter description

sh ./Scripts/copy.sh is static.

<username> specifies the user name of the remote Mac computer such as 'test'.

<ip_address> specifies the IP address of the remote Mac computer such as '10.10.0.0'.

Example: sh ./Scripts/copy.sh "test" "10.10.0.0"

5. Enter the password of the remote computer to connect to it.
6. Enter the command `sudo sh /tmp/install.sh`.
7. Enter the password of the remote computer when prompted.
8. Enter the command `exit` to close remote SSH session.
9. Repeat steps 4 through 8 to install Thirtyseven4 Mac Client Agent on a different remote computer.

Using PuTTY (for Windows OS)

The administrator computer having Windows OS can install Client Agent using this method.

Prerequisites

Before you install Thirtyseven4 Mac Client Agent, ensure the following requirements.

- Administrator must have an account on the Mac client computers with admin privileges.

- Enable Remote Login and either allow access for all users, or only for specific users, such as Administrators. You can find this setting on the Mac client computer under System Preferences > Sharing > Remote Login.
- Ensure that the firewall does not block the port that Secure Shell (SSH) uses, which is by default TCP port 22. This port allows the required communication for remote login.
- If you use the Mac firewall, disable stealth mode. With stealth mode enabled, the remote push installation cannot discover the client through Search Network.
- To disable stealth mode on the Mac computers, see the following Apple knowledge base article that applies to your version of the Mac operating system.
 - For 10.8, OS X Mountain Lion: see [Prevent others from discovering your computer](#).
 - For 10.9, OS X Mavericks: see [Prevent others from discovering your Mac](#).
 - For 10.10, OS X Yosemite: see [Prevent others from discovering your Mac](#).
 - For 10.11, OS X El Capitan: see [Prevent others from discovering your Mac](#).
 - For 10.12, macOS Sierra: see [Prevent others from discovering your Mac](#).
- Mac Thirtyseven4 Client installer must be created on the Thirtyseven4 Endpoint Security server. To know about how to create client installer, see [Creating the Mac Thirtyseven4 Client installer](#).

Installing Thirtyseven4 Mac Client Agent

To install Thirtyseven4 Mac Client Agent using PuTTY, follow these steps:

1. On the Thirtyseven4 Endpoint Security server, open cmd.exe and go to the folder “<installation directory>\Thirtyseven4\Endpoint Security 7.2\Admin\web\build\acmac”.
<installation directory> indicates the path where Thirtyseven4 Endpoint Security has been installed.
2. Enter the following command

```
.\Remote_Installation\Softwares\pscp.exe .\ MCCLAGNT.TAR .\Remote_Installation\Scripts\install.sh  

<username>@<ip_address>:/tmp/
```

Parameter description
<username> specifies the user name of the remote Mac client computer such as 'test'.
<ip_address> specifies the IP address of the remote Mac client computer such as '10.10.0.0'.
Example: .\Remote_Installation\Softwares\pscp.exe .\ MCCLAGNT.TAR
.\Remote_Installation\Scripts\install.sh test@10.10.0.0:/tmp/.
3. Open .\Remote_Installation\Softwares\putty.exe.
4. Enter the IP address of the remote Mac client computer and click Open.
5. In the PuTTY terminal Window, enter the user name and password of an administrator user on the remote computer.
6. Upon getting connected to the remote computer, type the following command `sudo sh /tmp/install.sh`.
7. Type the command `exit` to close SSH connection.

- Repeat steps 2 through 7 to install on a different Mac client computer.

Creating the Mac Thirtyseven4 Client Installer

To create the Mac Thirtyseven4 Client installer (.TAR file), follow these steps:

- On the Thirtyseven4 Endpoint Security server, go to **Start > Programs > Thirtyseven4 EPS Console > Client Packager**.
- In the Client Agent Package list, select **Custom**.
- In the OS Platform list, select **Mac**.
- Specify whether you want to include antivirus setup in Client Packager by selecting Yes or No from the Antivirus setup included list.

Select Yes if you want to include the antivirus setup in Client Packager. However, you cannot distribute this installer through email.

Select No if you do not want to include the antivirus setup in Client Packager. This installer can be distributed through email.

- Download the Mac Client build from the URL:

<http://updates.thirtyseven4.com/builds/2016/eps7.2/mclsetp.zip>

Copy and extract the downloaded build to "<installation_directory>\Thirtyseven4\Endpoint Security 7.2\Admin\Web\build\".

<installation_directory> indicates the path where Thirtyseven4 Endpoint Security has been installed.

- Click **Create**.

If you select Yes to include antivirus in the client packager, a MCCLAGAV.TAR file is created in the acmac folder.

If you select No to create client packager without antivirus, a MCCLAGNT.TAR file is created in the acmac folder.

- On Mac endpoint you need to copy and extract any of the above created TAR file and run the MCLAGNT.DMG file from the extracted folder to install Thirtyseven4 EPS Mac Client.

When the administrator downloads MCCLAGNT.TAR from the link provided in the email for 'Notify Install', the setup will be downloaded from the ACMAC folder of TSEPS server.



For roaming endpoints with MAC OS, only Custom client packager can be used for installing TSEPS client.

Disk Imaging

You can also deploy Endpoint Security client through disk imaging like Sysprep.

To deploy clients through Disk Imaging, follow these steps:

- 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:
 - Create a Client Packager without AV Build
 - 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 endpoint 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 endpoints. To avoid this, ensure that the Endpoint Security client does not communicate with the Endpoint Security server when it gets installed on the computer that is the source for disk imaging.



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

Firewall Exception Rules

Operating systems such as Windows has its own Firewall bundled with them. If the user prefers to retain the firewall bundled with the operating system, then exceptions can be created with Endpoint security for such systems. These exception rules are created during installation of Thirtyseven4 Endpoint Security. For the system on which Thirtyseven4 Endpoint Security is installed, the exceptions will be automatically created during installation. 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 7.2
- Client Agent 7.2
- Endpoint Security Site Port 7.2

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

- Client Agent 7.2

Remote Uninstall

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



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

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

1. Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Client Deployment > Remote Uninstall**.

The Remote Uninstall dialog appears that displays all the groups. Each group includes the name of the endpoints belonging to the group.

2. Select the endpoint from which you want to uninstall the Thirtyseven4 client. To uninstall Thirtyseven4 Client from all endpoints, select the check boxes available to the endpoint name columns.

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

3. Select Start Uninstall Notification.

The uninstallation starts.

Stop Uninstallation Notifications

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

1. Select the endpoints from which you want the clients should not be removed.
2. Click **Stop Uninstall Notification**.
3. 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.

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



Notification for Remote Uninstall from TSEPS web console will not be sent if the user is not logged on to the Mac system.

Chapter 7. Manage Groups

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

Adding a Group

To add a new group, follow these steps:

1. Log on to the 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.

Terms	Definition
Show endpoints within subgroup	Helps you display the endpoints that are in a subgroup.
Search	Helps you search an endpoint by its name or IP Address.
CSV	Helps you save the report in CSV format.



No subgroup can be created under the Default group.

Adding a Subgroup

To add a subgroup, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Manage Groups**.
2. Under TSEPS 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.

Deleting a Group

To delete a group, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Manage Groups**.
2. Under TSEPS 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 connected subgroups are also deleted.

Renaming a Group

To rename a group, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Manage Groups**.
2. Under TSEPS 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.

Importing from Active Directory

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

Note:

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

To import Active Directory Structure, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and select **Clients > Manage Groups**.
2. Under TSEPS Console, right-click a group.
Add Group, Delete Group, Rename Group, Import from Active Directory, and Set Policy options are displayed.
3. Select the Import from Active Directory option.
The Active Domain Controller dialog appears.
4. Select a domain and then click **Next**.
The authentication screen appears.
5. Type the user name in the format "domain name\user name" and then enter your password. Click **Next**.
6. On the Select Active Directory Container screen, select a Domain Name or Active Directory Container to import.
7. If you select a Domain Name, the whole Active Directory is imported and if you select any Active Directory Container, only the selected container is imported.
8. Click the **Finish** button.

Setting Policy to a Group

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

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

1. Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Manage Groups**.
2. Under TSEPS Console, select a group and then right-click it.
A submenu appears with the options such as Add Group, Delete Group, Rename Group, Import from Active Directory, and Set Policy.
3. Click the **Set Policy** option.
A list of policies appears.

4. Select the policy that you want to apply.

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

Changing Group of an Endpoint

Using this feature you can check if an endpoint should be in a certain group or the group has to be changed because of policy change at your organization. In case a change is incorporated, the protection policy of the new group will be applied.

To change the group of an endpoint, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Manage Groups**.

2. Under TSEPS Console, select a group.

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

3. Select an endpoint and drag it to a desired group where you want.

The endpoint is included in the new group.

Exporting groups and policies

This feature allows you to export groups and policies assigned to them from one TSEPS server to another. This is helpful when you need to move groups from one TSEPS server to another or in case of reinstallation. The data is downloaded to a .db file. You must copy that file to another server and use the import option to import groups and policies assigned to them.

To export groups and policies assigned to them, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and select **Clients > Manage Groups**.

2. Click **Export**.

A message is displayed, "Do you want to save or open this file".

3. Click **Save**.

The file containing groups and policies assigned to them is saved.

Importing groups and policies

This feature allows you to import entire groups and policies assigned to them from one TSEPS server to another. The groups' data is downloaded to a .db file when you export the groups. You must copy that file to another server and use the import option for groups.

To import groups, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and select **Clients > Manage Groups**.
2. Click **Import**.

The wizard to select a file appears

3. Select the file which is exported previously

The groups and policies assigned to them are imported and a message is displayed,

"File imported successfully".

Note: Policies, which are not assigned to any group, are not exported or imported from Manage Groups page. Those policies can be exported or imported by using Export or Import option on **Clients > Manage Policies page**.

Chapter 8. Manage Policies

Each organization prefers to enforce a policy that regulates its users. Thirtyseven4 Endpoint Security allows the administrators to create policies that help centrally control and manage the users belonging to a group.

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

Policies may include different client settings and scan schedules. Once a policy is created, it can be easily applied to a group. The users under a group or a subgroup will inherit the same policy. A group is nothing but a department in an organization. You should create groups before you create a policy setting. You can also view the policy status i.e. Applied, Pending or Failed on each client; this status can also be exported in .csv format.

To learn about how to create a group, see [Adding a Group](#).

Understanding Security Policy Scenario

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

Policy Settings for Marketing and Account Departments Compared			
Client Settings	Policy Features	Marketing Dept.	Accounts Dept.
Scan Settings	Scan mode	Automatic	Advanced
	Virus Protection Setting	Enabled	Enabled
	Block suspicious packed files	Enabled	Enabled
	Automatic Rogueware scan	Enabled	Enabled
	Disconnect Infected Endpoints 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
	Mobile Scan	Not 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
Advanced Device Control	Enable Advanced Device Control	Enabled	Enabled
	Device Types	No devices enabled	Devices selected and enabled
	Exceptions	Not enabled	Enabled and appropriately added
Data Loss Prevention	Enable Data Loss Prevention	Enabled	Enabled
	Select Data Transfer Channels	Monitor Network Share, Monitor Clipboard, Disable Print screen	Monitor Transfer through Application, Monitor Removable devices
	Select Data to be monitored	File Types, Confidential Data, User Defined Dictionaries	File Types, Confidential Data
	Actions	Block and Report	Report only
File Activity Monitor	Enable File Activity Monitor	Enabled	Enabled
	Removable Drives	Enabled	Enabled
	Network Drives	Enabled	Enabled
	Local Drives	Not Enabled	Enabled
Update Settings	Automatic update	Enabled	Enabled
	Download from Internet	Enabled	Not Enabled
	Download from Endpoint Security Server	Not Enabled	Enabled
Internet Settings	Proxy Settings	Enabled	Not Enabled
Patch Management	Scan and Install missing patches	Enabled	Enabled

General Settings	Authorize access to the client settings	Enabled	Enabled
-------------------------	---	---------	---------

Creating Policies

Policies help you manage client settings for different groups. You can create policies with client settings, and schedule settings to apply to different groups.

Creating a new policy

To create a new policy, follow these steps:

1. Log on to the 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. In the **Description** text box, enter brief details about the policy.
5. 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.

Note: If you enable this option, the Advanced Device Control and Data Loss Prevention features are disabled.

Copying a policy

To copy a policy, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and then select **Clients > Manage Policies**.
2. Select the policy that you want to copy and click **Copy Policy** icon.
The selected policy appears with its settings.
3. In the Policy Name text box, type the policy name.
You can also change the policy settings.
4. To save your setting, click **Save Policy**.

Renaming a policy

To rename a policy, follow these steps:

1. Log on to the 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 can also change the policy settings.

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

Deleting a policy

To delete a policy, follow these steps:

1. Log on to the 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

This feature allows you to import or export the policies of Thirtyseven4 Endpoint Security. If you need reinstallation or have multiple endpoints and want the same settings, you can simply export the settings configured on your current endpoint and easily import them on the endpoint(s). Both the default settings and the settings made by you can be exported.

Tip: The settings must be exported before you uninstall Thirtyseven4 Endpoint Security. Importing or exporting the settings can be done in the same way.

Exporting a policy

To export the policy settings, follow these steps:

1. Log on to the 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 the folder in which you want to store the policy.
4. Click **Save**.

The policy settings file is exported to the selected location.

Importing a policy

To import the policy settings, follow these steps:

1. Log on to the 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 message appears that allows you to select which policies you want to import.
4. Select the policies that you want to import and then click **Import**.

Chapter 9. Assets

Assets feature helps you keep a watch on the system information, hardware information, and software installed. You can also view the hardware changes if any that are made to the configuration of the systems in your network. You can also keep a tab on the list of the endpoints where the changes have actually been carried out and export the above information to a .csv file.

Viewing the details for Endpoints

To view the details follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Click **Clients > Assets**. The Assets view displays the following details of all the clients:

Fields	Description
Endpoint Name	Displays the name of the endpoint.
Group	Displays the group name to which the selected client belongs.
Domain	Displays the domain to which the selected client logs in.
IP Address	Displays the IP address.
Operating System	Displays the name of the operating system of the endpoint.
System Manufacturer	Displays the name of System Manufacturer.

To lookup the details for a particular endpoint, follow these steps

1. Do one of the following:
 - In the Assets page, enter the endpoint name/IP in the search text box and click the Search icon.
 - Select an endpoint from the displayed list.
2. Click **View Details**.

The View Details screen appears.

- The System Information tab displays the system information in details. OS Product key of the Windows OS appears.



The MS Office Product key is available only for MS Office 2010 and above.

- The Hardware Information tab displays the hardware information in details.
- The Software Installed tab displays the details of software installed on the system.

The MS Office Product key is available only for MS Office 2010 and above.



. The Product key of MS Office is not available in the clients with MAC operating system.

The license status of MS Office appears.

The following table mentions possible License status and their description for MS Office.

License status	Description
Unlicensed	The product is not licensed.
Licensed	The product is licensed.
OOBGrace	The MS Office license is in the grace period.
OOTGrace	The MS Office license requires reactivation.
NonGenuineGrace	The MS Office license has failed online validation and is in the grace period.
ExtendedGrace	The grace period of the MS Office license is extended.
Notification	The MS Office license is either out of the grace period or failed validation.

You can save the details of the endpoint in csv format.

Enabling Asset Management

You can enable the Asset Management reporting by the following procedure.

1. Log on to the **Thirtyseven4 Endpoint Security web console**.
2. Click **Admin Settings > Clients > Asset Management**.
3. To enable asset management, select the Enable Asset Management check box.
4. Click **Apply**.



The details of some softwares may not be displayed in Assets.

Chapter 10. Settings

This feature allows the administrators to see and customize the settings of the default policy. The default policy is available as soon as you install the product on your system. The default policy includes both the client settings and schedule scan settings and is optimal for security that you can apply to a group. However, you can customize the settings according to the requirement but its name cannot be changed. The default policy is also available in the Manage Policies option (**Thirtyseven4 Endpoint Security > Clients > Manage Policies**) from where you can customize its settings.

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

Client Settings

This section includes the following.

Scan Settings

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

The following table shows a comparison of the features in Scan Settings that are applicable for different 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 on to the Thirtyseven4 Endpoint Security web console and then select **Settings**.
2. On the Settings screen, click **Scan Settings**.
3. Under Scanner Settings, select the scan mode.

The Scan Mode includes Automatic and Advanced.

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

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

Scanner Settings

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

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

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



To know for which clients the features marked with asterisk are applicable, see the [comparison table](#).

Virus Protection Settings

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

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

Features	Clients	
	Windows	Mac
Load Virus Protection at Startup	✓	✓
Display alert messages	✓	✓
Report source of infection	✓	X
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.
Report source of infection	Displays the source IP address of the system where the virus is detected.
Select the action to be performed when a virus is found	<p>You can select an action that you want to take when a virus is found during manual scan. You can select any one of the following actions:</p> <ul style="list-style-type: none"> Repair – All the infected files are repaired automatically. The files that are not repairable are deleted. Delete – All the infected files are deleted automatically. Deny Access – Access to an infected file is blocked.

Advanced DNAScan Settings

Helps you safeguard the client systems even against new and unknown malicious threats whose signatures are not present in the virus definition database. DNAScan is an indigenous technology of Thirtyseven4 to detect and eliminate new types of malware in the system. DNAScan technology successfully traps suspected files with very less false alarms.

Advanced DNAScan Settings also includes the following:

Features	Description
Enable DNAScan	Helps in scanning the systems based on Digital Network Architecture (DNA) pattern.
Enable Behavior detection system	Helps in scanning the files and systems based on their behavior. If the files or systems behave suspiciously or their behavior changes by itself is considered as suspicious. This detection can be categorized based on their criticality level as Low, Moderate, and High. You can select the detection criticality level depending on how often suspicious files are reported in your systems.
Submit suspicious files	Helps in submitting suspicious files to the Thirtyseven4 research lab automatically for further analysis.
Show notification while submitting files	Displays a notification while submitting DNA suspicious files.



- The Advanced DNAScan Settings feature is available only in the clients with Windows operating systems.
- The 'Behavior detection system' scan setting is not applicable for Windows XP 64-bit and Windows Server platforms.

Block suspicious packed files

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

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



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

Automatic Rogueware Scan Settings

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



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

Disconnect Infected Endpoints from the network

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

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

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



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

Exclude Files and Folders

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

The following table shows a comparison of the features in Exclude Files and Folders that are applicable for different 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
Exclude from: Behavior Detection	✓	X

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

1. Log on to the 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 the Enter folder path text box.

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 text box.

5. Under Exclude from, select any option as per your requirement:
 - Known Virus Detection
 - DNAScan
 - Suspicious Packed Files Scan
 - Behavior Detection
6. To save your settings, click **OK**.

Important:

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

- If you select DNAScan, Suspicious Packed File Scan will also be enforced and both the options will be selected.
- However, you can select Suspicious Packed File Scan or Behavior Detection as a single option.

Exclude Extensions

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

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

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

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



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

Email Settings

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

The following table shows a comparison of the features in Email Settings that are applicable for different 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 on to the 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 settings, click **Save Policy**.

Email Protection

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

This feature is turned on by default which provides the optimal protection to the mailbox from malicious emails. We recommend that you always keep Email Protection turned on to ensure email protection. Once the feature is enabled, all incoming emails will be scanned before they are sent to Inbox.

To configure Email Protection, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Email Settings**.

The **Enable Email Protection** check box is selected by default.

3. The **Block attachments with multiple extensions** check box is selected by default. This option helps you block attachment in emails with multiple extensions. Worms commonly use multiple extensions which you can block using this feature.
4. The **Block emails crafted to exploit vulnerability** check box is selected by default. This option helps you block emails whose sole purpose is to exploit vulnerabilities of mail clients. Emails such as MIME, IFRAME contain vulnerability.
5. The **Enable attachment control** option helps you block email attachments with specific extensions or all extensions. If you select this option, the following options are enabled:
 - Block all attachments: Helps you block all types of attachments in emails.
 - Block user specified attachments: Helps you block email attachments with certain extensions. If you select this option, the Configure button is activated. For further settings, click Configure and set the following options:
 - a. In the User specified extensions dialog, select the extensions so that the email attachments with such extensions are blocked.
 - b. If certain extensions are not in the list that you want to block, type such extensions in the Extension text box and then click Add to add them in the list.
 - c. Click OK to save changes.
6. Select the **Enable Email scanning over SSL** check box to enable incoming mail scanning for mail accounts configured over SSL. Ensure that you perform the procedure to import the certificate for the mail client that you are using. This feature is available only in the clients with Microsoft Windows operating system.



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

Trusted Email Clients Protection

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

Trusted Email Clients Protection is an advanced option that authenticates email-sending application on the system before it sends the 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 includes Microsoft Outlook Express, Microsoft Outlook, Eudora, and Netscape Navigator.

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



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

Spam Protection

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

The following table shows a comparison of the features in Spam Protection that are applicable for different 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 on to the 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 from the following:
 - Soft:** Applies soft filtering spam protection policy.
 - Moderate:** Ensures optimum filtering. It is recommended to have moderate filtering enabled. However, this is selected by default.
 - **Strict:** Enforces strict filtering criteria. However, it is not ideal as it may even 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, see the [comparison table](#).

Setting spam protection rule for Whitelist

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

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

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Email Settings**.
3. Select the **Enable White List** check box.

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

4. 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 email 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 blacklist and whitelist.

Setting spam protection rule for Blacklist

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

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

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Email Settings**.
3. Select the **Enable black List** check box.

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

4. 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 email 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 blacklist and whitelist.

External Drives Settings

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

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

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

To configure External Drives Settings, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console and then click the **Settings** tab
2. Go to **Settings > Client Settings > External Drives Settings**.
3. Select the options that you want to enable.

The External Drives Settings options include: External Drives Settings, Autorun Protection Settings, and Mobile Scan Settings..

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

External Drives Settings

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

Autorun Protection Settings

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

Mobile Scan Settings

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

- USB Cable
- Bluetooth



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

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (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), etc. This detection implements a security layer to all communications and cordons your systems from unwanted intrusions or attack. You can also take actions like blocking the attackers for certain time, disconnecting the infected system from the network, and also send an alert message to the administrator.



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

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

1. Log on to the Thirtyseven4 Endpoint Security web console and then click the **Settings** tab
2. Go to **Settings > Client Settings > IDS/IPS**.
3. Enable one of the following options by selecting the check box:
 - Enable IDS/IPS
 - Detect Port Scanning Attack
On selecting this check box, Customize link is enabled.
 - Detect DDOS(Distributed Denial of Service) Attack
On selecting this check box, Customize link is enabled.
4. From the following options, select an action to be performed when attack is detected:
 - Block Attackers IP for ... Minutes.
Enter time here.
 - Disconnect endpoint from the network (only in case of DDOS and Port Scanning attack).
 - Display alert message when attack is detected.
This helps you take an appropriate action when attack is detected.
5. To save your settings, click **Save Policy**.

Customizing Port Scanning

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

1. Log on to the Thirtyseven4 Endpoint Security web console and then click the **Settings** tab

2. Go to **Settings > Client Settings > IDS/IPS**.
3. Select the **Detect Port Scanning Attack** check box.
The Customize link gets enabled.
4. Click the Customize link.
The Settings – Port Scanning dialog appears.
5. Select one of the following levels:
 - **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.
6. To exclude an IP address that you do not want to be scanned, click **Add** in Excluded IP Addresses section.
7. On the Add IP Address screen, type an IP Address or IP range and then click **OK**.
8. To exclude port that you do not want to be scanned, click **Add** from the Excluded Ports section.
9. 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. Log on to the Thirtyseven4 Endpoint Security web console and then click the **Settings** tab
2. Go to **Settings > Client Settings > IDS/IPS**.
3. Select the **Detect DDOS (Distributed Denial of Service) Attack** check box.
The Customize link gets enabled.
4. Click the Customize link.
The Settings – Denial of Service dialog appears.
5. Select one of the following levels:
 - **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.
6. To exclude an IP address that you do not want to be scanned, click **Add** in the Excluded IP Addresses section.
7. On the Add IP Address screen, type an IP Address or IP range and then click **OK**.

8. To exclude a port that you do not want to be scanned, click **Add** in the Excluded Ports section.
9. 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 connections. It analyzes all incoming connections whether it is secure and should be allowed through, and checks whether the outgoing communication follows the compliance that you have set for security policies. Firewall works silently in the background and monitors network activity for malicious behavior.

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



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

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. In the Level option, select one of the following:
 - Block all
 - High
 - Medium
 - Low
5. By default, the **Monitor Wi-Fi Networks** check box is selected. Because of this option, you get alert messages when connected with unsecured Wi-Fi network and when an attempt is detected to access unsecured client Wi-Fi (hotspot). Also the reports are generated at the server.
6. If you want an alert message about firewall violation, select the **Display alert message when firewall violation occurs** check box.
7. If you want reports for all blocked connections, select the **Enable firewall reports** check box.
8. In the Exceptions section, a list of default exceptions appear. You can add or manage the exceptions. For more information, see Managing Exceptions.
9. To restore the default settings, click the **Default** button.

10. To save your settings, 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 connection.

Security Level

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

Managing the Exceptions rule

With Exceptions, you can allow genuine programs to perform communication irrespective of the Firewall level whether set as High or Medium. With Exceptions, you can block or allow Inbound and Outbound communication, through IP Addresses and Ports.

Creating the Exception rule

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. In Exceptions section, click **Add**.
5. On the Add/Edit Exception screen, type a name in the Exception Name text box and select a protocol.
The protocol includes TCP, UDP, and ICMP.
6. Click **Next**.

7. Under Local 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.

8. Under Local 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. If you mention Local IP Address or IP range or port, this exception will be applicable for incoming communications.

9. Under Remote 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. If you mention remote IP or port, that exception will be for outgoing communications.

10. Under Remote 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.

11. Under Action, select either **Allow** or **Deny**.

12. Click **Finish**.

The Exception is added at top position in the Exceptions list. The sequence of the exceptions decides the precedence of the rule. The precedence is in descending order. You can move the exception rule with the **Move Up** and **Move Down** buttons.

13. Click **Save Policy**.

Editing the Exceptions rule

You can edit the exceptions rule which are created by you if required. To edit the Exceptions rule, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security Web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. In Exceptions section, select the exception that you want to edit.
5. On the Add/Edit Exception screen, you can edit the name in the Exception Name text box and edit the protocol.

The protocol includes: TCP, UDP, and ICMP.

6. Click **Next**.
7. Edit Local IP Address if required, and then click **Next**.
8. Edit Local TCP/UDP Ports if required, and then click **Next**.
9. Edit Remote IP Address if required, and then click **Next**.
10. Edit Remote TCP/UDP Ports if required, and then click **Next**.
11. Under Action, you can select either **Allow** or **Deny**.
12. Click **Finish**.

13. Click **Save Policy**.

Deleting the Exceptions rule

You can delete the exceptions rule that you created. To delete the Exceptions rule, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security Web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. In Exceptions section, select the exception that you want to delete.
5. Click **Delete**.

The selected exception rule is deleted.

6. Click **Save Policy**.

Exporting the Exceptions rule

You can export the exceptions rule that you created. To export the Exceptions rule, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security Web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. In Exceptions section, select the exception that you want to export.
5. Click **Export**.

The Opening fwexcp.db dialog appears.

6. Select **Save File**.

7. Click **Ok**.

The database file, fwexcp.db is downloaded.

Importing the exceptions rule

You can import the exceptions rule that you created in the earlier versions of TSEPS. To import the Exceptions rule, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security Web console.
2. Go to **Settings > Client Settings > Firewall**.
3. To enable Firewall, select the **Enable Firewall** check box.
4. Click **Import**.

The File Upload dialog appears.

5. Select the database file, fwexcp.db.

6. Click **Open**.

The database file, fwexcp.db is imported.

7. Click **Save Policy**.

Web Security

This feature helps you create security policies for a department or group where Browsing and Phishing Protection can be enabled. This blocks malicious and phishing Web sites. You can also restrict or allow access to the Web sites 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 Web sites (Web Categories)	✓	✓
Block specified Web sites	✓	✓

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Web Security**.
3. Under Web Security, select either of the following or both the check boxes:
 - Browsing Protection
 - Phishing Protection
4. To get an alert message when a blocked Web site is accessed by a user, select the **Display alert message when Web site is blocked** check box.
5. Under Web Categories, restrict or allow access to the Web sites based on their categories as per the security policy of your organization. To enable the categories, select the **Restrict access to particular categories of Web sites** check box.

If you block a category, all the Web sites under it will be blocked.
6. In Block specified websites section, enter the Web sites that you want to block. This is helpful if you are sure to block certain Web sites. To enable this section, select the **Restrict access to particular Web sites** check box.
7. To schedule the internet access, select the **Schedule Internet Access** check box and do the following:
 - i. Select one of the following options:
 - Always allow access to the internet

- Restrict internet access

When you select the option, **Allow access to the internet**, you can add the schedule.

- ii. Click **Add** to add the schedule.
Add Time Interval dialog appears.
- iii. Select the **Weekday** from the list.
- iv. Select the **Start at** and **End at** hours.
- v. Click **OK**.

You can delete the schedule entry if the entry is not required.

8. You can exclude certain known websites from getting it blocked. Excluded URLs/Websites will not get blocked even if internet is restricted. To exclude the websites, do the following,
 - i. Select the **Schedule Internet Access** check box.
 - ii. Select the **Restrict internet access** option.
 - iii. Click **Exclusions**. The Exclude URLs dialog appears.
 - iv. Enter complete URL that you want to exclude.
 - v. Click **Add**.
 - vi. Click **Ok**.

The list of excluded URLs is displayed in the Excluded URL box.

You can delete the URL entry if the entry is not required.



SSL versions earlier than 3.1 are not supported for Schedule Internet Access.

9. Select the **Enable Web Security reports** check box if you want to generate reports for all blocked Web sites.

If you select this option, a large number of reports will be generated depending upon the Web usage.

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



The Schedule Internet Access feature is available only in the clients with Microsoft Windows and Mac operating systems.

Browsing Protection Settings

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

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

Phishing Protection Settings

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

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

Exclusion for Browsing Protection and Phishing Protection

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

You can exclude the URLs in the following way:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Web Security**.
3. In the Web Security section, click the **Exclusion** button.

The Exclude URLs dialog appears

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

The Report Miscategorized URL dialog appears. You can report about miscategorization of the URL to the Thirtyseven4 lab if the URL is detected as malicious or a phishing site.

5. Select one of the reasons from the following:

URL is getting detected as Malicious.

URL is getting detected as Phish.

6. 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.

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

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

Web Categories

There are certain concerns that most organizations may face:

- System infection by malware.

- Users browsing unwanted Web sites.
- The employees idling away time.

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

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

To configure Web Categories, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Web Security**.
3. Under Web Categories, select the **Restrict access to particular categories of Web sites** check box.

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

4. From Status column, select either **Allow** or **Deny**.

Exclusion for Web Categories

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

You can enlist such Web sites in the Exclusion list in the following way:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Web Security**.
3. In Web Categories section, select the **Restrict access to particular categories of Websites** check box.
4. Click the **Exclusion** button.

The Exclude URLs dialog appears

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

The URL is added in the Exclude URL list.

6. To exclude the subdomains, select the **Also Exclude Subdomains** check box.
7. To save your settings, click **OK**.

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

Block specified websites

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

To block Web sites, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Web Security**.
3. On the Web Security screen, under Block specified websites section, select the **Restrict access to particular Websites** check box.

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

4. To add a Web site, click **Add**.
5. On the Add URL screen, type a URL in the Enter URL text box.

*If you want to block the subdomains, select the **Also Block Subdomains** check box. 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.*

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



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

Application Control

Organizations usually face the following concerns while using applications:

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

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

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



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

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

1. Log on to the **Thirtyseven4 Endpoint Security web console**.
2. Go to **Settings > Client Settings > Application Control**.

3. To block access to an application, select the **Block unauthorized application when accessed** check box.
4. If you want to send a notification when a blocked application is accessed, select **Notify clients** when an unauthorized application is blocked.
5. Select either Authorized or Unauthorized to each application category as per your requirement.

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

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

Custom

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

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

You can customize the applications in the following way:

1. Log on to the **Thirtyseven4 Endpoint Security web console**.
2. Go to **Settings > Client Settings > Application Control**.
3. Under Application Control, click **Custom** to an application category.

Ensure that the option Block unauthorized application when accessed is selected, only then you can click the Custom option.

A list of applications under the selected application category appears

4. In the list of applications, select all application names that you want to mark as unauthorized.
5. To save your setting, click **Save Policy**.

Add Application

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

To add an application, do the following:

1. Log on to the **Thirtyseven4 Endpoint Security web console**.
2. Go to **Settings > Client Settings > Application Control**.
3. In the Add Application section, click the **Custom Applications** button.
4. On the Custom Applications screen, click **Add Application**.
5. Browse and give the path to the application.

6. In the Application Name text box, type an application name.
7. 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 to improve the quality of the software product.

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

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

Submit Application metadata to Thirtyseven4 lab

With this option, you can send metadata of an application to the Thirtyseven4 lab for including it in the application categories. Metadata includes information of application such as its Name, Version, Company Name, and MD5. You can also provide the reason for adding the application. This information will help us to improve the Application Control module.

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

However, if you have unauthorized an application category but an application is not yet blocked, you can submit that application. Thirtyseven4 analyzes the application and then enlists it in the category.

Note:

- User may get application blocked prompt even while copying or renaming any unauthorized application.
- Some unauthorized applications may start in case the application executable is updated due to software update. Such applications can be added to Endpoint Security Console and you are recommended to submit the Metadata to the Thirtyseven4 lab.

Advanced Device Control

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

- Autorun feature does not activate any infection.
- Unnecessary data or applications do not clog the systems.

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



On Windows 2000 and Windows XP SP1 and later operating systems, you will not be able to block devices other than USB storage devices.

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Advanced Device Control**.

3. To enable device control, select the **Enable Advanced Device Control** check box.
4. Under Select Access Policy for Device Types section, select a category from the following options:
 - Storage Device
 - Card Readers
 - Wireless
 - Mobile & Portable devices
 - Interface
 - Camera
 - Others
5. For the corresponding device under that category select one of the following:
 - Block
 - Allow
 - Read only

Note: Options under any category are available only if you select the main category check box.

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

This policy is applied to all the devices that are configured in the list. Even if you add a device, the same policy will apply unless you customize the policy.

For Windows Clients

- Only NTFS is supported for Partial encryption..
- 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.
- USB devices connected to the systems in the network of TSEPS 7.2 server will not be enumerated in **Admin Settings > Server > Manage Devices > Add Devices > Network Devices** list.
- Some devices (e.g.,: Nokia phones, BlackBerry phones) may need system reboot or device reattachment for device access rights to be applied.
- On blocking SATA Controller from Advanced Device Control, you may frequently see SATA Controller blocked prompts even when actual blocking is not performed.

- While any ongoing session of Webcam or Bluetooth is in progress, changing access right to block will not interrupt this current ongoing session. The device may need reattachment or system reboot for access rights to be applied.
- External CD/DVD reader will not be enumerated in **Admin Settings > Server > Manage Devices > Add Devices > Network Devices** list and also exception rule cannot be created for the same.

For Mac Clients

- If the option Read only is selected in Advanced Device Control of TSEPS and a USB device is attached, such a device may not be accessible from the left pane in Finder for some time.
- If a USB device is already attached to the machine and you are installing Mac client, the device may not be shown as mounted for a fraction of seconds.
- If an NTFS USB device is attached to the machine during installation of Mac client, two copies of the attached USB may be visible for a few seconds.
- If a USB device is to be shown as mounted or un-mounted using terminal commands, the Device Control policy will not apply to that device.
- If you are installing Mac client on Mac OSx 10.9 while an FAT USB device is attached to the machine, such a device will not be displayed as mounted. To show the device mounted, you need to disconnect the device and reconnect it.
- iDevices, Internal Card Reader, Webcam, CD-DVD, mobile phones and HFS encrypted devices may need device reattachment for device access rights to be applied.
- Exception functionality will not be applicable for Bluetooth, Wi-Fi, Webcam, External CD-DVD.
- Mobile phones except iDevices that are connected in 'USB Mass Storage' mode will be detected under USB storage device category.
- Mobile phones connected in MTP mode will be detected under 'Windows Portable Devices' category.
- USB storage device won't be formatted with Mac OS extended (Journaled, Encrypted) file format.
- If block permission is set to i-devices, then i-devices will not get blocked when connected to the Mac system. This is applicable only for Mac OS 10.12.

Adding exceptions to the device control list

You can add exceptions for removable devices that are used by authorized persons so that the devices are excluded from the policy.

To add devices to the exceptions list you must first authorize the devices by adding the device to the server, as follows,

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Admin Settings > Server > Manage Devices**.

3. Click **Add Devices**.
4. Select from Network Devices, USB Devices, or Other Devices.
If you want to add a USB Device, select USB Device and in the Add Device dialog box, add the device name and click OK.
If you want to add a network device, select Network Devices. The list of devices detected in the network is displayed. Select the device and click OK.
If you want to add any other device, select the Other Device option, select device type, and in the Add Device dialog box, add the required details such as Device name, Device Vendor ID, Product ID, and the serial number. Click OK,
5. Click **Settings > Client Settings > Advanced Device Control**. Ensure that the option for Enable Advanced Device Control is selected.
6. Click Exceptions.
7. Click **Add**.
8. Select one or more devices to add to exception from the devices displayed in the list.
9. Click **OK**.
10. Click **Yes** to the Managed Devices confirmation dialog box.
11. Set the access permissions as required.
12. Click **Save Policy**.
If you add the same device from 'USB by Model' option and also from 'USB devices' option and set 'Block/Allow/Read Only' permissions to both types of devices, then the permission set of 'USB by Model' device takes the priority.

Adding Device to Server

To know about how to add a device to the server, see [Manage Devices](#).

Data Loss Prevention

You can now prevent unauthorized loss, pilferage, or leakage of confidential company data using the Data Loss Prevention (DLP) feature of the TSEPS 7.2.

It is necessary to enable DLP on the endpoints. To do this, see [Enabling DLP feature](#).

You can also view a report of the users who attempted to cause the unauthorized leakage of confidential data. See [Reports for Data Loss Prevention](#) for more information.

The DLP feature can stop any such unauthorized activity that is carried out through the following channels:

- Using the Print Screen option to save the screenshot (Applicable only for Windows platform). The file/data is not monitored.
- Using Removable Devices to copy data (Applicable only for Windows platform)
For selected File Types, the Removable Devices go to 'Read Only' mode when 'Monitor Removable Devices' option is selected.

- Using Network Share accessed using UNC Path or Mapped Network Drive (Applicable only for Windows platform)
- Using the Clipboard to paste information from one application to another
- Using printer activity, printing through local and network printer. The file/data is not monitored. (Applicable only for Windows platform)
- Using online services of third-party Application/Services to send data such as email, file sharing apps, cloud services, Web browsers and other applications using social media

You can also identify the type of data that you want to monitor such as:

1. File Types

- Graphic Files (Audio, Video, Images)
- Office Files (MS Office, Open Office, Kingsoft Office)
- Programming Files
- Some Other File Types (Compressed files etc.)
- Custom Extension Files

2. Confidential Data

- Confidential data such as Credit/Debit Cards
- Personal information such as Social Security Number (SSN), Email ID, Phone Numbers, Driving License Number, Health Insurance Number, Passport Number, ID, International Banking Account Number (IBAN), Individual My Number and Corporate My Number, Pin Code, Aadhar Number and Vehicle Registration Number.

3. User Defined Dictionary

To specify the words/strings that must be flagged if used in communication.

Note:

Confidential Data & User Defined Dictionary Data will not be monitored and blocked if it is in the Subject Line or Message Body of email, instant messenger communication.

You can either choose to be notified through email notification when an attempt is made to leak information, or prevent the attempt from being carried out successfully.

Note:

- *Data Loss Prevention feature is not available in both TSEPS Business and Total flavor. User need to purchase a DLP pack separately to avail this feature.*
- *Data Loss Prevention feature is not supported with the TSEPS SME flavor.*
- *DLP feature is not available on Windows 2000 Operating System.*

Preventing leakage of data

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client settings > Data Loss Prevention.**

Select the option to enable Data Loss Prevention. You can choose to select the option for an Alert message on the endpoint on which an attempt is made at data leakage.

3. Select the channels that you want to monitor from the following:
 - Disable Print Screen (applicable only in Windows platforms)
 - Monitor Removable Devices (applicable only in Windows platforms)
 - Monitor Network Share (applicable only in Windows platforms)
 - Monitor Clipboard
 - Printer Activity (applicable only in Windows platforms)
 - Monitor Data Transfers through Application/Online Services
4. Select the applications that you want to monitor for attempts at data pilferage by clicking on the Applications drop down list. Do one of the following:

You can select all the applications in the group

- Select the applications one by one after expanding the group caret.
 - Select all Mac platform applications by clicking the Mac group icon.
 - Select all Windows applications by clicking on the Windows icon.
 - Select all Web Browsers or one by one after expanding the group caret.
 - Select all E-mail applications or one by one after expanding the group caret.
 - Select all Instant Messaging applications or one by one after expanding the group caret.
 - Select all File Sharing/Cloud Services applications or one by one after expanding the group caret.
 - Select All Social Media/Others applications or one by one after expanding the group caret.
5. To configure email SSL settings, select the **Enable Email scanning over SSL** check box. This is applicable only when you select Email option in the Application / Online Service. Ensure that you perform the procedure to import the certificate for the mail client that you are using. This feature is available only in the clients with Microsoft Windows operating system.
 6. Configure the settings for File Types, Confidential Data, and User Defined Dictionary.
 7. Configure the action to be performed after the attempts are carried out, for example Block and Report or Report only.

Alert prompts will not be displayed for Report Only action.

8. In the Configure Exceptions section, do the following:
 - i. In the Domains tab, select the **Enable domain Exception** check box.
 - ii. Select the domains to exclude from Data Loss Prevention.
 - iii. In the Applications tab, select the **Enable applications Exception** check box.
 - iv. Select the applications to exclude from Data Loss Prevention.

- v. In the Network Share tab, select the **Enable Network Share Exception** check box.
- vi. Select the network share to exclude from Data Loss Prevention.

9. Click **Save Policy**.



For Mac Client:

- Confidential & User Dictionary Data will not be blocked in subject line, message body of email or messenger communication.
- Prompts and report will be generated in case if monitored file type is downloaded.
- Certain file types (POT, PPT, PPTX, DOC, DOCx, XLS, XLSX, RTF) containing unicode data will not be blocked.
- Thirtyseven4 provides you an advanced scanning feature, Data-At-Rest Scan. With this feature you can search for a particular type of data in various formats.

File Activity Monitor

This feature lets you monitor any suspicious activity related to the confidential files on your computer, a network drive or a removable drive. Apart from a default set of files, you can customize and select the file types that you want to monitor. You can monitor the selected file types for actions such as copy, delete, or rename. You can generate a report for the file activity from the Reports page.



The File Activity Monitor feature is available in the clients with Windows and Mac operating systems.

Enabling File Activity Monitor

To enable file activity monitor follow the given steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > File Activity Monitor**.
3. Select **Enable File Activity Monitor**.
4. In the **Select File Types and Events to monitor within drives** section, Select the drives that you want to monitor for file activity.
Note: Selection of event is not applicable for Removable Drives, Network Drives. You can select to monitor only 'delete' activity for local drives. For Removable Drives you can select 'All Files' to be monitored.
5. In the File types list, select the file types that you want to monitor for all the drive types or you can select all the file types listed by using 'All File Types' check box.
6. In the Custom Files, you can add your own file types that you want to exclude. Click the plus sign (+) to add a new file type extension to be monitored. Use the delete icon to remove a file or folder type.
7. Enter the folder paths that you want to exclude from the monitoring, for example. C:\JSmith.
To remove a folder path from the exclusions, click on the delete icon, which appears when you click the list entry. If you click on the delete icon, a message box is displayed to confirm the delete action.

- Click **Save Policy**.

Update Settings

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

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

The following table shows a comparison of the features in Update Settings that are applicable for different 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:

- Log on to the Thirtyseven4 Endpoint Security web console.
- Go to **Settings > Client Settings > Update Settings**.
- To take the updates automatically, select **Enable Automatic Update**.
- To display notification window when the updates are taken, select **Show update notification window**.
- 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.

- Under Update Mode, when TSEPS is installed on private IP (Private IP natted to Public IP), the following update settings can be configured:

For local clients

- Download from Internet
- Download from Endpoint Security Server
- Download from Specified Update Servers

For remote clients

- Download from Internet

- Download from Specified Update Servers

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

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

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



- If 'Update from Internet' option is enabled (by right clicking on Virus Protection icon at system tray) on client, the client will try to take the updates first from the Endpoint Security Server. If the server is not reachable, the updates will be automatically taken from the Internet Center.
- 'Update from Internet' feature is available only in the clients with Microsoft Windows and Mac operating systems.
- To know for which clients the asterisk features are applicable, see the [comparison table](#).

Entering update server locations

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

To enter a server location, follow these steps:

1. On the Thirtyseven4 Endpoint Security Dashboard, click **Home**.
2. On the Home page, click the **Update Manager** link, available next to the product name and version details.
3. On the Update Manager screen, click **Alternate Update Managers**.
4. In the Enter Update Manager URL text box, type a **URL** and then click **Add**.

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

Internet Settings

This feature gives the administrators a wider choice of creating policies for the client modules that need Internet connection to function. You can configure different settings for the server and port so that the client modules such as Quick Update, Spam Protection, Web Security, and Messenger have Internet connection. This is very helpful in allowing the client modules to function in a secure work environment where default Internet connection is not allowed.

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > Internet Settings**.
3. To set the proxy setting for Internet, select **Enable Proxy Setting**.

The proxy settings details are activated.

4. In Proxy Server, type the sever name.
5. In Port, type the port number.

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

6. To save your setting, click Save Policy.



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

Patch Server

This feature allows you to configure the patch server to check and install the missing patches.

To create a policy with patch server settings, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security Web console.
2. Go to **Settings > Client Settings > Patch server**.
3. Select the **Enable Patch Server** check box.
4. Select the patch server from the list that will be used by the endpoint to check and install the missing patches.
5. Select the **Use Microsoft patch server for roaming endpoints to scan missing patches and installing them** check box.
6. To save your setting, click **Save Policy**.

The Patch Server feature is applicable only for the clients with Microsoft Windows OS; does not support Mac operating system.

General Settings

This feature allows you to create a policy that authorizes the clients to access client settings and change their own password, enable or disable Safe Mode Protection, 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 Safe Mode Protection	✓	X
Enable Self Protection	✓	X
Enable News Alert	✓	X

Enable Backup data	✓	X
--------------------	---	---

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Client Settings > 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 Safe Mode Protection, select Enable Safe Mode Protection*.
6. To activate Self Protection, select **Enable Self Protection***.
7. To get the news alert about various incidents, select **Enable News** alert*.
8. The **Enable Backup Data** check box is selected by default. This feature automatically and periodically (multiple times a day) takes a backup of all your important and confidential files present on the endpoint. If you update any file then this feature automatically takes backup of the latest copy.

Backup of the following file types is maintained:

.doc, .odp, .txt, .docx, .ods, .wps, .dps, .odt, .wpt, .dpt, .pdf, .xls, .et, .ppt, .xlsx, .ett, .pptx, .odg, .rtf, .docm, .xlsm and .pptm

Disable this feature if you have any other provision for data backup (Example: File server backup, Data backup server, etc.)

9. To save your setting, click Save Policy.



To know for which clients the asterisked features are applicable, see the [comparison table](#).

Schedule Settings

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

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

You can schedule scanning for the following.

Client Scan

This feature allows you to create policies to initiate scanning the clients automatically at a convenient time. You can define whether the scan should run daily or weekly, select scan mode (Quick Scan, Full System Scan). You can also enable Antimalware while scanning. This will

supplement other automatic protection features to ensure that the client systems remain malware-free.

The following table shows a comparison of the features in Client Scan that are applicable for different 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 on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Schedule Settings > Client Scan**.
3. Configure the following settings: Client Schedule Scan, Scanner Settings, and Antimalware Scan Settings.
4. To save your settings, click **Save Policy**.

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

Client Schedule Scan

This feature helps you define scan schedules for the clients at a certain frequency.

To configure Client Schedule Scan, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Schedule Settings > Client Scan**.
3. Under Client Schedule Scan section, select **Enable Schedule Scan**
4. In Frequency, select either the Daily or Weekly option.
5. In Start At, set time in hours and minutes.
6. If you want to repeat scanning of your clients, select **Repeat Scan** and set the frequency after what interval the scan should be repeated.
7. To get notification when a client is offline, select **Notify if client is off-line**.

Scanner Settings

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

To configure **Scanner Settings**, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Schedule Settings > Client Scan**.
3. In Scanner Settings section, under How to Scan, select a scan mode from the following:

- **Quick Scan** (Scan Drive where operating system is installed)
 - **Full System Scan** (Scan all the fixed drives)
4. To set optimal setting, select the **Automatic** option.
 5. 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.
 6. 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
 7. 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, and Skip.
 8. In Select action to be performed when a virus is found, select an action from the following: Repair, Delete, and Skip.

Antimalware Scan Settings

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

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



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

Application Control

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

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Schedule Settings > Application Control**.
3. Configure the following settings: Application Control Schedule Scan, and Scan and Report.
4. To save your setting, click **Save Policy**.

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



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

Application Control Schedule Scan

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

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

Scan and Report

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

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

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

Tuneup

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

To create a policy for Tuneup, follow these steps:

1. Configure the following settings: Tuneup Schedule Scan and Tuneup Settings.
2. To save your setting, click **Save Policy**.

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



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

Tuneup Schedule Scan

This feature helps you define schedules to tune up the clients at the preferred frequency.

To configure **Tuneup Schedule Scan**, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Schedule Settings > Tuneup**.
3. Under Tuneup Schedule Scan, select the **Enable Schedule Tuneup** check box.

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

Tuneup Settings

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

- Disk cleanup
- Registry cleanup
- Defragment at next boot

Vulnerability Scan

This feature helps you schedule vulnerability scan for the clients so that the clients are scanned for possible vulnerabilities.

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Schedule Settings> Vulnerability Scan**.
3. Configure the following settings: Vulnerability 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 Vulnerability Scan feature is available only in the clients with Windows operating systems.

Scheduling Vulnerability Scan

This feature helps you define schedules to initiate vulnerability scan of the clients as per your convenience.

To schedule Vulnerability Scan, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Settings > Schedule Settings> Vulnerability Scan**.
3. Under Vulnerability Scan, select the **Enable Schedule Scan** check box.
4. In Weekday, select a day of the week.
5. In Start At, set time in hours and minutes.
6. If you want to repeat scanning, select **Repeat Scan** and then set the frequency after what interval the scan should be repeated.
7. To get notification when a client is offline, select the **Notify if client is off-line** check box.

Scan and Report

Under Scan and Report, select any of the following:

- Microsoft applications and other vendor applications
- Microsoft applications only
- Other vendor applications only

Data-At-Rest Scan

With this feature you can search for a particular type of data in various formats and detect any confidential data that is present in your endpoints and removable devices. To know more, see [Data-At-Rest Scan](#).

To perform Data-At-Rest scan, you must enable DLP on the endpoints. To do this, see [Enabling DLP feature](#).

To create a policy for Data-At-Rest Scan, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security Web console .
2. Go to **Settings > Schedule Settings > Data-At-Rest Scan**.
3. Select Enable Schedule Scan and set the frequency and time for the scan.
You can choose to Repeat Scan and Notify if client is offline.
4. To save your setting, click **Save Policy**.

Patch Scan

The patch scan checks for the missing patches of the installed products and operating system (OS) on the client machine. After the check is complete, the result is generated.

To create a policy for patch scan, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security Web console .
2. Go to **Settings > Schedule Settings > Patch Scan**.
3. Select the **Enable Automatic Patch Scan** check box and set the frequency and time for the scan.

You may also select **Notify if client is offline**.

4. In the Patch Install Settings section, select **the Automatic Install missing software patches with severity level equal to or more than:** check box and then select the severity level from the list.
5. Select the **Allow auto-restart the system** check box.
6. To exclude endpoints from installing the patches, click the **click here** link.

Exclusion for Patch Install dialog appears.

- i. You can select the Exclude endpoints having Server OS in an TSEPS network check box if required.

- ii. Select the **Exclude below endpoints** check box.
 - iii. Enter endpoint name or IP.
 - iv. Click **Add**. The endpoint details appear. You can remove the endpoint. To remove, select the endpoint from the list and click **Remove**.
 - v. Click **Apply**.
7. To save your setting, click **Save Policy**.

Chapter 11. Reports

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

Client

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

Viewing Reports of Virus Scan

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

To view reports of Virus Scan, follow these steps:

1. Log on to the **Thirtyseven4 Endpoint Security** web console and then click the **Reports** tab
2. Go to **Reports > Client > Virus Scan**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group Name and an Endpoint Name.

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

5. Enter user name in the **User Name** text box.
6. Select the **Report Type**.

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

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

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click Modify Parameters.

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:

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

Viewing Reports of AntiMalware Scan

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

To view reports of Antimalware Scan, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > Client > AntiMalware Scan**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group Name and an Endpoint Name.

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

5. Enter user name in the **User Name** text box.
6. Select the **Report Type**.

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

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

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click Modify Parameters.

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:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.

User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Name of Malware	Displays the malware names.
Type of Malware	Displays the malware types.
Action Taken	Displays the actions that were taken against the malware attack.

Viewing Reports of Web Security

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

To view reports of Web Security, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > Client > Web Security**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a group name and an endpoint name.

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

5. Enter user name in the **User Name** text box.
6. Select the **Report Type**.

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

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

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click Modify Parameters.

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

Note: In case of SME and 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:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Blocked Web sites	Displays the Web sites that were blocked.
Category	Displays the category of the blocked Web sites belong to.

Viewing Reports of Tuneup

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

To view Tuneup reports, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > Client > Tuneup**.

The reports are displayed in the chart format.

3. To generate reports for a group, select the **Group Name**.
4. Enter user name in the **User Name** text box.
5. Select the **Report Type**.

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

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

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click Modify Parameters.

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 save it as csv or PDF.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when Tuneup is performed.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Tuneup Status	Displays whether the client was tuned up.
Last Performed	Displays when last Tuneup was performed.

Viewing Reports of Advanced Device Control

This feature helps you 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 > Advanced Device Control**).

To view reports of Advanced Device Control, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > Client > Advanced Device Control**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group Name and an Endpoint Name.

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

5. Enter user name in the **User Name** text box.

6. Select the **Report Type**.

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

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

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click Modify Parameters.

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.



Device Control prompts and reports will not be generated for "Network Share".

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

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
User Name	Displays the user name that belongs to the domain.
Device Name	Displays the device name that breached the policy.
Device Type	Displays the device type of the device.
Serial Number	Displays the serial number of the device.
Action Taken	Displays the action that was taken against the violation of the Device Control policy.

Viewing Reports for Data Loss Prevention (DLP)

This feature helps you generate and view reports related to attempts at pilfering or copying data in an unauthorized manner. The report pinpoints the user, endpoint on which the attempt was carried out, the time and channel of operation.

On Access Scan

To receive the data for specific time period with the help of On Access Scan, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > Client > Data Loss Prevention > On Access Scan**.
3. Enter the start date and end date for the period for which you want the data.
4. Select the **Group name**.
5. Enter the endpoint name.

6. Enter user name in the **User Name** text box.
7. Select the **Report Type** i.e. Chart or Tabular.
8. Select the channel through which the suspected activity might be carried out.
9. Click **Generate**.

*After clicking Generate button, a summary is displayed. If you want to change the parameters, click **Modify Parameters**.*



Prompts and reports will not be generated for "Disable Print Screen" functionality.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the start date of the report.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the name of the domain.
User Name	Displays the name of the user.
IP Address	Displays the IP address of the endpoint.
Source	Displays the path of the file from where its data was copied or accessed.
Content Type	Displays the type of content which was accessed.
Matched Item	Displays the subtype of content which was accessed.
File Path	Displays the path of the file from where its data was copied or accessed.
Channel	Displays the channel through which the suspected activity was carried out.
Channel Details	Displays the details of the channel through which the suspected activity was carried out.
Sender	Displays the email ID of the sender.
Receiver	Displays the email ID of the receiver.
Subject	Displays the subject of the email.
Action Taken	Displays the action taken to monitor the suspected activity.

On Demand/Schedule Scan

This scan generates and lets you view a report for confidential information and user defined dictionaries in the selected endpoints. The report also displays matching text as per your search criteria that is found while scanning. For more information about how to scan, see [Data-At-Rest Scan](#).

1. Log on to the Thirtyseven4 Endpoint Security Web console.
2. Go to **Reports > Client > Data Loss Prevention > On Demand/Schedule Scan**.
3. Enter the start date and end date for the period for which you want the data.
4. Select the Group Name and enter the Endpoint Name.
5. Enter user name in the **User Name** text box.
6. Select Report Type i.e. Chart or Tabular.
7. Select the type of content to be scanned.
8. Click **Generate**.

You can print or export the report in csv or PDF formats.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the name of the domain.
User Name	Displays the name of the user.
Scan Type	Displays the type of scan, either On Demand or Schedule Scan.
Confidential Data Incidents	Displays the total number of confidential data located when scanning.
Data Dictionary Incidents	Displays the total number of user defined dictionary data located when scanning.
Details	Displays the details of Data-At-Rest scan.

Viewing Reports for Application Control

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

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

On Access Scan

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > Client > Application Control**.
3. On the General Reports page, click the **On Access Scan** tab to generate reports of the applications that were accessed.
4. Select the start and end dates for the reports.
5. Select a **Group Name** and an Endpoint Name.

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

6. Enter user name in the **User Name** text box.
7. Select the **Report Type**.

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

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

After clicking Generate button, Collapsible Summary will be displayed. In addition, if you want to change the parameters then you can do it by using Modify Parameters button.

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:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
User Name	Displays the user name that belongs to the domain.
Blocked Application	Displays the applications that were blocked.
Application Version	Displays the version of the applications that were blocked.
Application Category	Displays the category of the blocked applications.
Application Path	Displays the path of the blocked applications where they were installed.

Application Installed

To view reports for Application Installed, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console
2. Go to **Reports > Client > Application Control**.
3. On the Generate Reports page, click the **Application Installed** tab to generate reports.
4. Select the start and end dates for the reports.
5. Select a Group Name and an Endpoint Name.

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

6. Enter user name in the **User Name** text box.
7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, Collapsible Summary will be displayed. In addition, if you want to change the parameters then you can do it by using Modify Parameters button.

You can take the print of the generated report or can also save the report as csv or PDF using the respective buttons.

This report page displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Group Name	Displays the group name that the selected client belongs.
Module Name	Displays the module name that scanned the applications.
Summary	Displays the summary of the installed applications.
View Details	Displays further details of the installed applications. To view the details, click the View Details link. It also includes information of what authorized and unauthorized applications are present on client machine.

Viewing Reports of IDS/IPS

This feature helps you generate reports on whether there was any Port scanning attack, DDOS (Distributed Denial of Service) attack, or any attempt of intrusion, and what actions were taken.

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > Client > IDS/IPS**.
3. On the General Reports page, select the start and end dates for the reports.
4. Select a Group name and an Endpoint name.

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

5. Enter user name in the **User Name** text box.
6. 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.

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

After clicking Generate button, Collapsible Summary will be displayed. In addition, if you want to change the parameters then you can do it by using Modify Parameters button.

You can take the print of the generated report or can also save the report as csv or PDF using the respective buttons.

This report page on Intrusion Prevention displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.

User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Vulnerability Detected	Displays the vulnerability detected in a client.
Action Taken	Displays the actions that were taken against the attack.
View Details	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:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Attacker IP	Displays the IP address of the attacker.
Attacker MAC Address	Displays the MAC address of the attacker.
Scanned Ports	Displays the Ports that were scanned.
Action Taken	Displays the actions that were taken against the attack

This report page on DDOS displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Attacker IP	Displays the IP address of the attacker.
Attacker MAC Address	Displays the MAC address of the attacker.
Action Taken	Displays the actions that were taken against the attack.

Viewing Reports of Firewall

This feature helps you generate reports on the protection policy for Firewall such as the blocked connection for communications (Inbound or Outbound) and Firewall security level (**Settings > Client Settings > Firewall**).

To view reports of Firewall, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console
2. Go to **Reports > Client > Firewall**.
3. On the General Reports page, click the **firewall** tab to generate reports.

4. Select the start and end dates for the reports.
5. Select a Group name and an Endpoint name.

If you want to generate a report for a group, leave the endpoint name text box blank. If you want to generate a report for an endpoint name, select the group name and then type an endpoint name. The report will be generated for the endpoint name that belongs to the selected group.

6. Enter user name in the **User Name** text box.
7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, Collapsible Summary will be displayed. In addition, if you want to change the parameters then you can do it by using Modify Parameters button.

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

This report page on Firewall displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Local IP	Displays the local IP address.
Remote IP	Displays the remote IP address.
Protocol	Displays the Protocol name.
Direction	Displays the direction of the blocked communication connection.
Firewall Level	Displays the level of the Firewall security policy.
View Details	Displays further details of the installed applications. To view the details, click the View Details link.

Viewing Reports of Wi-Fi

This feature helps you generate reports about the Wi-Fi connection. The reports gives details about the endpoints when connected to unsafe Wi-Fi.

To view reports of Wi-Fi, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security Web console.
2. Go to **Reports > Client > Firewall**.
3. On the Generate Reports page, click the Wi-Fi tab to generate reports.
4. Select the start and end dates for the reports.
5. Select a Group name and an Endpoint name.

If you want to generate a report for a group, leave the endpoint name text box blank. If you want to generate a report for an endpoint name, select the group name and then type an

endpoint name. The report will be generated for the endpoint name that belongs to the selected group.

6. Enter user name in the **User Name** text box.
7. To generate the report on the selected parameters, click **Generate**.

Collapsible Summary appears. Moreover, you can change the parameters by using **Modify Parameters** button.

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

This report page on Wi-Fi displays the following details of the clients.

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Wi-Fi Name	Displays the name of the Wi-Fi connection.
Physical Address	Displays the physical address of the endpoint.
Events	Displays the event when connected to unsecured Wi-Fi. Example: Connection to unsafe Wi-Fi detected.

Viewing Reports of Vulnerability Scan

This feature helps you generate reports on vulnerabilities present in the endpoints in the network. Reports can be filtered based on any of the following categories:

- All Vulnerability
- Severity
- Vendor
- Top Vulnerability

To view reports of Vulnerability Scan, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > Client > Vulnerability Scan**.
3. On the Generate Reports page, select the start and end dates for the reports.
4. Select a Group name and an Endpoint name.

If you want to generate a report for a group, leave the endpoint name text box blank. If you want to generate a report for an endpoint name, select the group name and then type an endpoint name. The report will be generated for the endpoint name that belongs to the selected group.

5. Enter user name in the **User Name** text box.

6. In Report Type, select the type of report you want to generate.
7. To generate the report on the selected parameters, click **Generate**.

After clicking Generate button, Collapsible Summary will be displayed. In addition, if you want to change the parameters then you can do it by using Modify Parameters button.

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

This report page on Vulnerability Scan displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Vulnerability ID	Displays the unique CVE-ID of a vulnerability incident.
Vulnerability Title	Displays the description of a vulnerability incident.
Severity	Displays the criticality of a vulnerability incident.
Vendor	Displays the name of a vendor from where the vulnerability is reported.
View Details	Displays further details of the vulnerability. To view the details, click the View Details link.

Viewing Reports for File Activity Monitor

This feature lets you view reports for suspicious file activity as per the configured settings. You can generate the reports using the following parameters:

- Start date
- End date
- Location
- Group name
- Endpoint name
- Event

Reports are available in a tabular format or a pie chart format. The report also displays the information about the attempts made, the name of the user, the endpoint name and the number of incidents for all the local, network or removable drives. You can click on the link above the charts to view the file type split up against locations. You can also view a summary of the activity for a particular file type such as deleting a file. You can view the file activity related to a person.

Viewing reports for file activity

1. Log on to the Thirtyseven4 Endpoint Security web console

2. Go to **Reports > Clients > File Activity Monitor**
3. In the Generate Reports section, enter the start date and end dates between which you want to monitor file activity.
4. Select the location, group name, Endpoint name and the type of event you want to monitor.
5. Enter user name in the **User Name** text box.
6. Click **Generate**. The report is generated and displayed on the screen. You can switch between a tabular view and a pie-chart view.

After clicking Generate button, a collapsible summary is displayed. If you want to change the parameters, click Modify Parameters.

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

This report page for File Activity Monitor displays the following details of the clients:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
File Name	Displays the file name, which is being monitored.
Location	Displays the type of Drive.
User Name	Displays the user name that belongs to the domain.
Details	Displays the details of the event.

Viewing Reports for Asset Management

The Asset Management tab on the Reports page lets you generate reports related to the assets or the Endpoints. You can generate these reports for a particular period, group-wise, or for a particular Endpoint. Reports are available in a bar and chart format. You can also choose the category of report required, i.e. a hardware changes report or a software changes report. You can print these reports if required.

Viewing reports for asset management

Asset Incidents

To view asset management reports, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports> Client > Asset Management**.
3. Select the **Asset Incidents** tab.

In the Generate Reports area, enter or select the criteria for the required report. You can generate a report for a particular period, or select the type of report required, or look up the report for a particular endpoint by entering the name of the endpoint in the corresponding field.

4. Enter user name in the **User Name** text box.
5. Select the **Report type**, whether bar chart or tabular.
6. Click **Generate**. The report is displayed on the screen. Use the Print icon if you want to print the report.

Current Assets

To view current asset reports, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports> Client > Asset Management**.
3. Select the Current Asset tab.
4. In the Generate Reports area, enter or select the criteria for the required report. Select the Operating System, System Manufacturer, Processor, Last Shutdown Before, RAM or Application Name.

Click **Generate**. The report is displayed on the screen. Use the Print icon if you want to print the report. You can also save the report as csv or PDF.

Viewing Reports of Patch Management

This feature helps you generate reports about the patches. The reports display details about the patches installed on the endpoints in the network.

You can generate the reports using the following parameters:

- Start date
- End date
- Group name
- Endpoint name
- Report Type
- Severity
- Patch status

Reports are available client wise or patch wise in a tabular format. The report also displays the information about the domain, name of the patch, name of the application, vulnerabilities targeted, scan type, and patch status. You can also view the details of the patch.

To view reports of patches, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security Web console.
2. Go to **Reports > Client > Patch Management**.
3. Select the start and end dates for the reports.
4. Select a Group name.

If you want to generate a report for a group, leave the endpoint name text box blank. If you want to generate a report for an endpoint name, select the group name and then type an

endpoint name. The report will be generated for the endpoint name that belongs to the selected group.

5. Enter user name in the **User Name** text box.
6. Select **Report Type**, **Severity** and **Patch Status**.
7. To generate the report on the selected parameters, click **Generate**.

A summary report appears. Moreover, you can change the parameters by using **Modify Parameters** button.

You can print the report by clicking the **Print** option. You can also save the report as csv or PDF format.

8. To view the patch details, click the **Patch Title** link.

Patch Details dialog appears. You can print the patch details by clicking the Print option. You can also save the patch details as csv or PDF format.

9. Click **Close**.

The patch-wise report page displays the following patch details:

Fields	Description
Date and Time	Displays the date and time when the report is generated.
Endpoint Name	Displays the name of the endpoint for which the report is generated.
User Name	Displays the name of the user.
Domain	Displays the domain to which the selected client logs in.
Patch Title	Displays the name of the patch in the hyperlink format. You can click the name to view details of the patch.
Severity	Displays the severity of the missing patch.
Category	Displays the category of the installed patch.
Application	Displays the name of the application. Example, Windows 8
Vulnerabilities Targeted	Displays the vulnerability targeted in a client.
Scan Type	Displays the type of scan.
Patch Status	Displays status of the patch.

The client-wise report page displays the following patch details:

Fields	Description
Endpoint Name	Displays the name of the endpoint for which the report is generated.
Domain	Displays the domain to which the selected client logs in.
Scanned Patches	Displays the count of scanned patches. <ol style="list-style-type: none"> 1. To view the list of scanned patches, click the count. The list of scanned patches appear in a new dialog. 2. To view the patch details, click the Patch Title link.

	<ol style="list-style-type: none"> 3. Patch Details dialog appears. You can print the patch details by clicking the Print option. You can also save the patch details as csv or PDF format. 4. Click Close to close the window.
Installed Patches	<p>Displays the count of installed patches.</p> <ol style="list-style-type: none"> 1. To view the list of installed patches, click the count. The list of installed patches appear in a new dialog. 2. To view the patch details, click the Patch Title link. 3. Patch Details dialog appears. You can print the patch details by clicking the Print option. You can also save the patch details as csv or PDF format. 4. Click Close to close the window.
Installation Failed	<p>Displays the count of failed installation of patches.</p> <ol style="list-style-type: none"> 1. To view the list of failed installed patches, click the count. The list of failed installed patches along with installation error message appear in a new dialog. 2. To view the patch details, click the Patch Title link. 3. Patch Details dialog appears. You can print the patch details by clicking the Print option. You can also save the patch details as csv or PDF format. 4. Click Close to close the window.

Server

This feature helps you check the event logs of all the incidents that took place on server. The OTP generation logs for temporary device access also appears.

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

1. Log on to the Thirtyseven4 Endpoint Security web console
2. Go to **Reports > Server**.
3. Select the start and end dates for the reports.
4. On the Event Logs page, select the category for the reports.

You can print the report or save the report as csv or PDF format using their respective buttons. You can also delete the event logs, if you prefer.

Fields	Description
Delete	Helps you delete the event logs.
Print	Helps you take the print of the event logs.
csv	Helps you save the report in csv format.
PDF	Helps you save the report in PDF format.

Manage

This feature helps you manage the reports generated on server and client. You can set when the reports can be removed automatically. You can also export the reports and delete them manually.

Managing Settings

This feature helps you set when to remove the reports automatically in the following way:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > Manage > Settings**.
3. On the Settings page, set the following:
 - In Automatically delete reports older than...days, set the number of days when the reports should be deleted automatically.
 - In Automatically email reports for past... days 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**.

Note: If any module contains more than 1000 records, then only latest 1000 records will be emailed.

Managing Export

This feature helps you export the reports in PDF in the following way:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > 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 an endpoint 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

This feature helps you delete the reports manually in the following way:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Reports > Manage > Delete Reports**.

3. Under Manually delete reports, select one of the following options:
 - Delete reports older than ...days: Select the number of days to remove the reports older than the days you want to.
 - Delete all reports: Select this option if you want to remove all the reports generated till now.
4. Under Select Reports, select the report types that you want to remove from the following:
 - Clients Reports
 - Server Reports
5. After setting the criteria, click **Delete** to remove the reports.

Chapter 12. **Admin Settings**

The Admin Settings section includes the following topics:

Server

This feature allows you to configure various settings related to server. 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.

Change Password

To prevent unauthorized users from modifying your settings or removing the Thirtyseven4 client from endpoints 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 on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Admin Settings > 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 retype the new password in the Confirm Password text box.
5. Click **Apply**.

Change Email Address

Here you can see your registered Email address. If required, you can change the Email address.

To change the Email address, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Admin Settings > Server > Change Email Address**.
3. In the **Email Address** text box, edit the Email Address.
4. Click **Apply**.

Notification

This feature helps you set rules for sending notifications for various events such as when virus is detected, virus is active in memory, virus outbreak or ransomware detected on endpoints.

Notifications are sent against intrusion detection, if an unauthorized device or application is accessed or virus definitions get outdated. This also includes alerts for failure of synchronization

with Active Directory, or any license related information etc. Notifications keep you informed about the incidents occurring across the network so that appropriate action can be taken to avoid any mishap.

Notification includes the following:

- Email Notification for various incidents.
- Configure Email for Event Notification for creating a list of Email IDs.

Email Notification

To configure Email Notification, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Admin Settings > 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 mediums through which you want to get the notification for the following incidents:
 - Virus detected on endpoint
 - Virus active on endpoint
 - Virus outbreak in network
 - Ransomware detected on endpoints

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 IDS/IPS, select the events for which you want to get notifications:
 - Intrusion detected on endpoint
 - Port Scanning incident detected on endpoint
 - DDOS Attack detected on endpoint.

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

6. Under Advanced Device Control, select the events for which you want to get notifications:

- Attempt to breach the Device Control policy

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

7. Under Application Control, select the events for which you want to get notifications:

- Attempt to access unauthorized application

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

8. Under Update, select the medium through which you want to get the notification for the following incidents:

- Service pack is available
- Endpoints are not updated with the latest virus definitions
- Virus definitions of Update Manager are outdated

Note: The notification for Endpoints are not updated event can be sent through email only.

9. Under Install through Active Directory, select the medium through which you want to get the notification for the following incidents:

- Synchronization with Active Directory failed

10. Under Disconnected Endpoints, select the events for which you want to get notification:

- Endpoint disconnected from the network due to infection
- Endpoint disconnected from the network due to DDOS Attack
- Endpoint disconnected from the network due to Port Scan

Note: The notification for all incidents can be sent through email only.

11. Under License related, select the medium through which you want to get notification for any of the following incidents:

- License expired
- License is about to expire
- License limit exceeds

12. Under Data Loss Prevention, enable notification for event:

Attempt to breach Data Loss Prevention policy.

13. Under Asset Management, enable notification for event

Hardware changes made in the Endpoint.

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

Configuring Email for Event Notification

To configure Email Event Notification, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web.
2. Go to **Admin Settings > Server > Notification**.

3. In Configure Email for **Event Notification**, click **Configure**.

The Email Notification prompt appears.

4. In the List of Email IDs, type an email address and then click **Add**.

You can enter multiple email addresses.

5. To save the email addresses, click **Apply**.

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

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

SMTP Settings

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

To configure the SMTP Settings, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Admin Settings > Server > SMTP Settings**.
3. In the SMTP Server text box, type the IP Address or domain name of SMTP server.
4. In the Port text box, type the port number.
5. In the Notify from Email Address text box, type the email address.

This email address will appear as From Address in all the emails sent from TSEPS server.

6. For user authentication, type the user name in the **User name** text box.

The User name field depends on your SMTP server. It may ask you to provide either user name or email ID.

7. In the **Password** text box, type the password.
8. In User Authentication Method, select one of the following:
 - None: Select this option to send email notification through HTTP protocol.
 - SSL: Select this option to send email notification through SSL (Secure Sockets Layer) protocol.
 - TLS: Select this option to send email notification through TLS (Transport Layer Security) protocol.
9. We recommends that to ensure the SMTP host details are correct, test the SMTP settings. To test the SMTP settings, click **Apply**, and then click **Test SMTP Settings**.
10. In the Test Mail dialog, in the **To** text box, enter the email ID of the user.
11. Click **Send Mail**.

TSEPS cannot send emails if the SMTP settings are configured using public mail server (Example: Gmail) and if Allow less secure apps setting is disabled in the public mail servers.

Manage Devices

This feature helps you to authorize all USB Devices and system internal devices (Example: Bluetooth, Webcam). Authorized devices can be allowed or blocked at TSEPS client system when configured through policy. This authorization must be done for every USB storage device to manage the devices in the TSEPS environment.

Cleaning USB device

Before adding a device to the Device Control tool (dcconfig tool), clean the disk.

To clean the disk, follow these steps:

1. Connect the device.
2. On the command prompt, type the following commands one by one:

diskpart

list disk

Select disk <#>

Clean

convert mbr

3. After clean up, create partition on the disk.

Now the disk is ready to be added.

Viewing details of devices

To view details of devices, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security Web console.
2. Go to Admin Settings > Server > Manage Devices.
3. A list appears which contains devices which can be added to the device exceptions in Device Control settings.

The list displays the following details of the devices:

Fields	Description
Device Name	Displays the device name.
Device Type	Displays the device type of the device.
Endpoint Name	Displays the name of the endpoint.
Serial Number	Displays the serial number of the device.
Model Name	Displays the model name of the device.
Encryption Status	Displays one of the following encryption type of the devices, <ul style="list-style-type: none"> • Not encrypted • Partially encrypted • Fully encrypted
Authorized	Displays status of the encryption, whether Yes / No

Adding device where TSEPS client is installed/ not installed

To add the device where TSEPS client is installed/ not installed, follow these steps:

1. Log on to the Web console.
2. Connect the clean device.
3. Go to **Admin Settings > Server > Manage Devices**.
4. Select **Add Devices > USB Devices**. Add Device dialog appears.
5. Click the link **click here** to download Device Control devices package.
6. Extract the zip file DEVCTRL.7Z.
7. From the devctrl folder, double click the dcconfig.exe file.
8. The device details appears in the Device control dialog. In the Device name box, enter device name.
9. To authorize the device, do one of the following:
 - If you are using the system where the TSEPS client is installed, the available encryption options are:
 - No encryption
 - Partial encryption
 - Full encryption
 - If you are using the system where the TSEPS client is not installed, the available encryption options are:
 - No encryption
 - Partial encryption
 - To apply the encryption, refer the following table:

Encryption	Description
No	<ul style="list-style-type: none"> • Clear the Make this device accessible only within your corporate network check box. This is selected by default. • Clear the Encrypt this device check box.
Partial	<ul style="list-style-type: none"> • Select the Make this device accessible only within your corporate network check box. This is selected by default. • Clear the Encrypt this device check box.
Full	<ul style="list-style-type: none"> • Select the Make this device accessible only within your corporate network check box. This is selected by default. • Select the Encrypt this device check box. • When you apply the full encryption, Format window appears. Format the device.

10. Click **Add**.

Partial encryption supports only NTFS. No encryption and full encryption supports all the file systems.

Adding exceptions to the device control policy

You can add exceptions for removable devices that are used by authorized persons so that the devices are excluded from the policy.

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Admin Settings > Server > Manage Devices**.
3. Click the device category from the **Add Devices** drop down list. The following device categories are displayed:
 - **Network Device:** A list of devices connected to the network is displayed. Select the devices that you want to manage. Click **OK**.
 - **USB Devices:** Use this option if you want to add a USB device that is not in the Network Device list and not connected. For more information, see TSEPS server is installed or Adding device where TSEPS client is installed/ not installed.
 - **USB by Model:** Use this option if your organization has a large number of USB storage devices of the same make and model. You can add these USBs by model name. The Add device by Model Name dialog box appears. Enter the Device Name. Select a mode from the “Add Model Name list box. The following modes are displayed:
 - **Automatically:** The device model name is automatically displayed if a USB mass storage device is attached to Windows operating system.
 - Automatically fetching of model name is not supported on Mac operating system.
 - **From the list:** A list of pre-specified device model names appears. Select a model name from the list.
 - **Manually:** Enter **Model Name**. Follow the procedure mentioned on the dialog box.
 - If same USB storage device is authorized as USB Device and USB by Model, the priority will be given to the Model name.
 - **Other devices:** Use this option if you want to add a device that is not connected, and not in the list. Select the device type and enter the corresponding details for that device.
4. Select the devices that you want to manage from the displayed list and click **OK**.

After the device appears in the list, toggle the button under Authorized to Yes or No as required. You can also use the Edit icon that appears to change the device name as it appears or use the Trashbox icon to delete the device from the list.

***Note:** If you set the device authorized permission to ‘No’, then that device cannot be added to the exceptions list.*
5. To add the device to the exceptions list, go to **Settings > Client Settings > Advanced Device Control**.
6. Click **Exceptions**.
7. Click **Add**. The Managed Devices dialog box displays the list of authorized devices.

8. Toggle the **Add to Exceptions** button for that device.
9. Click **OK**.
10. Click **Yes** on the Managed Devices confirmation dialog box. The device is now added in the list of exceptions.

To delete a device, select the device, and then click the Trash icon that appears.

11. Set the access permissions as required.
12. Click **Save Policy**.



- In case you are accessing Web console on Windows Vista, turn off the 'Protected Mode' option in Internet Explorer.
- If you are unable to add devices through the Web console, you can also use the Device Control Tool to add USB Storage devices. This tool is available at the following location on the TSEPS Server: <Installation folder>\Admin\dcconfig.exe.
- Add device functionality will not work with Edge browser on Windows 10 operating system and on Google Chrome 44 and later versions.

Data Loss Prevention

For Data Loss Prevention, you can do the global settings for the following features:

- User Defined Dictionary
- Domain Exceptions
- Custom Extensions
- Application Exceptions
- Network share Exceptions

User Defined Dictionary

You can add certain key words, or phrases that might contain, or refer to confidential information in the User Defined Dictionary. If any of the documents on your endpoints contains the text or phrase that you have added to the User Defined Dictionary, the Data-At-Rest Scan or [Data Loss Prevention](#) feature displays the path or location of these documents.

Adding Dictionary

To add dictionary, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > User Defined Dictionary**.
3. Click **Add Dictionary**.
4. Enter the details such as name, description and the word that you want to add.
5. Click **Add**.

You can add multiple words to the dictionary.

You can also delete a word from the list by selecting a particular word and clicking Delete.

6. Click **OK**.

Importing Dictionary

You can also import a dictionary that you prefer to use.

To import the dictionary, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > User Defined Dictionary**.
3. Click **Import**.
4. In the Import Dictionary dialog, click **Browse**.

The File Upload dialog appears.

5. Select the valid exported dictionary database file (Example: expdict.db).
6. Click **Open**.

The database file is imported.

Exporting Dictionary

You can export a dictionary that you have created.

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > User Defined Dictionary**.
3. On the User Defined Dictionary page, select the dictionary that you want to export.
4. From the Actions column, click **Export** icon.

The database file is downloaded. The default name of the database file is expdict.db. If required, you can change the filename.

Actions on Dictionary

You can edit, delete or export the added dictionary by selecting the dictionary from the provided list and performing the required action from the Actions column.

Domain Exceptions

In this section, you can add the domain names that you want to exclude from Data Loss Prevention.

Domain Exceptions support the Windows platform.

Adding domain name

To add a domain name to exclude from Data Loss Prevention, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Domain Exceptions**.
3. Enter the domain name in the text box.

4. Click **Add**.

Deleting domain name

- To delete an individual domain name, click the Delete icon available next to the domain name.
- To delete multiple domain names, select the check boxes of the domain names that you want to delete, and then click Delete.

Importing domain name

You can import a domain name that you prefer to use.

To import the domain name, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Domain Exceptions**.
3. On the Domain Exceptions page, Click **Import**.

The File Upload dialog appears.

4. Select the valid exported domain database file (Example: exdomain.db).
5. Click **Open**.

The database file is imported.

Exporting domain name

You can export a domain name that you created.

To export the domain name, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Domain Exceptions**.
3. On the Domain Exceptions page, select the domain name that you want to export.
4. Click **Export**.

The database file is downloaded. The default name of the database file is exdomain.db. If required, you can change the filename.

Actions on domain name

You can also edit, or delete the added domain name by selecting the domain name from the provided list and performing the required action from the Actions column.

Custom Extensions

In addition to the default extensions of the files, you can monitor other extensions as per your requirement. These additional extensions are called Custom Extensions.

In this section, you can add the Custom Extensions to monitor from Data Loss Prevention.

Custom Extensions support the Windows platform only.

Adding Custom Extensions

To add Custom Extensions, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Custom Extensions**.
3. Enter Custom Extensions.
4. Click **Add**.

Deleting Custom Extensions

- To delete an individual Custom Extensions, click the **Delete** icon available next to the Custom Extensions.
- To delete multiple Custom Extensions, select the check boxes of the Custom Extensions that you want to delete, and then click **Delete**.

Importing Custom Extensions

You can import a Custom Extension file that you prefer to use.

To import a Custom Extension file, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Custom Extensions**.
3. On the Custom Extensions page, Click **Import**.

The File Upload dialog appears.

4. Select a valid Custom Extension database file (Example: expfiles.db).
5. Click **Open**.

The database file is imported.

Exporting Custom Extensions

You can export a Custom Extensions that you have created.

To export a Custom Extension file, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Custom Extensions**.
3. On the Custom Extensions page, select the Custom Extension that you want to export.
4. Click **Export**.

The database file is downloaded. The default name of the database file is expfiles.db. If required, you can change the filename.

Actions on Custom Extensions

You can also edit, or delete the added Custom Extensions by selecting the Custom Extension files from the provided list and performing the required action from the Actions column.

Application Exceptions

In this section, you can add an application to exclude from Data Loss Prevention. Add only those applications which are monitored by Data Loss Prevention.

Application Exception supports the Windows platform only.

Adding Application Exceptions

To add Application Exception, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Application Exceptions**.
3. To add an application, click **Browse** and provide complete path to the application.
4. Enter the application name.
5. Click **Add**.

If you are adding an application from system32 folder on X64 bit OS, copy that application from system32 folder to any other location. Then add the application from that location.

Deleting Application Exceptions

- To delete an individual Application Exception, click the Delete icon available next to the Application Exception.
- To delete multiple Application Exceptions, select the check boxes of the Application Exceptions that you want to delete, and then click Delete.

Importing Application Exceptions

You can import an Application Exception that you prefer to use.

To import the Application Exception, follow these steps,

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Application Exceptions**.
3. On the Application Exceptions page, Click **Import**.

The File Upload dialog appears.

4. Select a valid exported application database file (Example: expapps.db).
5. Click **Open**.

The database file is imported.

Exporting Application Exceptions

You can export an Application Exception that you created.

To export the Application Exception, follow these steps:

1. On the Application Exception page, select the application that you want to export.
2. Click **Export**.

The database file is downloaded. The default name of the database file is expapps.db. If required, you can change the filename.

Actions on Application Exceptions

You can also edit, or delete the added Application Exceptions by selecting the Application Exceptions from the provided list and performing the required action from the Actions column.

Network share Exception

In this section, you can add a network share path in UNC format to exclude from Data Loss Prevention.

Adding Network share Exception

To add Network share Exception, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to Admin Settings > Server > Data Loss Prevention > Network share Exception.
3. Enter the Network share Exception.
4. Click Add.

Deleting Network share Exception

- To delete an individual Network share Exception, click the Delete icon available next to the Network share Exception.
- To delete multiple Network share Exception, select the check boxes of the Network share Exception that you want to delete, and then click Delete.

Importing Network share Exception

You can import a Network share Exception that you prefer to use.

To import the Network share Exception, follow these steps,

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Server > Data Loss Prevention > Network share Exception**.
3. On the Network share Exception page, Click **Import**.
The File Upload dialog appears.
4. Select a valid exported network share database file (Example: expnetsh.db).
5. Click **Open**.

The database file is imported.

Exporting Network share Exception

You can export a Network share Exception that you created.

To export the Network share Exception, follow these steps:

1. On the Network share Exception page, select the application that you want to export.

2. Click **Export**.

The database file is downloaded. The default name of the database file is expnetsh.db. If required, you can change the filename.

Actions on Network share Exception

You can also edit, or delete the added Network share Exception by selecting the Network share Exception from the provided list and performing the required action from the Actions column.

Network share Exception supports the Windows platform only.

Redirection

This feature helps you change the TSEPS Server for upgrading your TSEPS to new version. This helps in redirecting the existing clients to new TSEPS Server and thereby using the new TSEPS Server for communication. You can select the clients or configure all of the clients to be redirected to the new server. This feature is particularly useful in cases of large networks where the clients are connected through low bandwidth lines. You can use this feature to move the clients in groups selectively to the new server so that redirection is gradual and at your convenience.

In case of software version upgrade, the previous version TSEPS Client will get uninstalled and new version of TSEPS Client will get installed.

The following table explains the supported redirection cases,

EPS Server of earlier version	EPS Server of higher version
Installed on local/private IP	Installed on local/private IP
Installed on local/private IP	Installed on local/private Domain
Installed on local IP (natted with public)	Installed on local IP (natted with public)
Installed on public IP	Installed on public IP
Installed on public IP	Installed on FQDN(Fully qualified Domain Name)



- When the redirection process is in progress, the previously installed TSEPS should not be uninstalled. If you uninstall the previous TSEPS before the redirection process command is delivered to all the clients, then the clients who fail to receive the command will neither communicate with previous TSEPS nor with the new TSEPS.
- Group Revival: To maintain the earlier client group-policy structure after client redirection, administrator can export the older client group-policy structure from Manage Groups and import it in new TSEPS server. After redirection old client will be placed in the same group as earlier on new TSEPS server.
- If group with same name is present on redirected server then newly imported group is renamed with suffix "_1".
- Group revival is applicable for MAC and Windows clients only.

To configure Redirection, follow these steps:

1. Log on to the **Thirtyseven4 Endpoint Security web console**.
2. Go to **Admin Settings > Server > Redirection**.
3. In the **Server Name/IP** text box, type the sever name or IP address.
4. In the **Port** text box, type the Port number.
5. Do the following:
 - i. Select the **Select this check box to add a public IP address/Hostname** check box.
 - ii. Only In case of remote clients, in the Server Name/IP text box, type the sever name or public/natted IP address of new TSEPS server.

If TSEPS is installed through public mode then the above two fields do not appear.
6. Select one option from Redirection Type list:
 - Select all clients: To select all the clients which are to be redirected.
 - Redirect and Auto-Reboot all clients: To redirect all the clients and auto-reboot them during upgrade process. Enabling this option would prompt user with 15 minutes countdown reboot prompt, and a forceful reboot will occur after 15 minutes. After the client reboot, the new version of Client will be installed (silently) and complete the redirection process.
 - Redirect selected clients: If you select this option, you can select specific clients for redirection process. On selecting this option, the Select Clients link is displayed. Click Select clients. In the Select Clients dialog box, select the clients that you want to redirect and click OK. Use the Endpoint name\IP search box on the upper-right corner to search for endpoints by name or IP address.
7. To apply your settings, click **Apply**.



Client system will not reboot automatically if the redirection process is carried out for same TSEPS version even if the Redirect and Auto-Reboot all clients option has been configured.

Manage Users

This feature helps you create, edit, disable and delete 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. A Super Administrator can create and modify Administrator users. Only the Super Administrator has the privilege to uninstall Thirtyseven4 Endpoint Security.

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

Administrator

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

1. Such a user cannot create another user with Administrator privileges.
2. Such a user cannot uninstall Thirtyseven4 Endpoint Security.

Report Viewer

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

Creating New Users

To create a new user, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Admin Settings > Server > Manage Users**.
3. On the Manage Users page, click **Add User**.
An Add/Edit User dialog 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, retype the new password.
7. In the **Email ID** text box, type the email Id of the user.
8. From the **Type** list, select the user type.
The user type includes Administrator and Report Viewer.
9. Select to enable or disable the user from the **User Status** list.
10. To save the settings, click **Save**.

Modifying Existing Users

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

1. Log on to the Thirtyseven4 Endpoint Security web console
2. Go to **Admin Settings > Server > Manage Users**.
A list of all users appears.
3. Click the **Edit** button next to the user that you want to edit.
4. You can modify the setting according to the right privileges assigned to you.
The Add/Edit User dialog appears.
5. In the New Password text box, type the new password.
6. In the Confirm New Password text box, retype the new password.
7. From the Type list, select the new type if you want.
8. Select to enable or disable the user from the **User Status** dropdown.
9. To save you settings, click **Save**.

Deleting Users

To delete an existing user, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to Admin Settings > **Server** > **Manage Users**.

A list of all users appears.

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

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

A confirmation message appears.

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

Internet Settings

This feature gives the administrators to use proxy settings for server modules that need an Internet connection to work. You can configure the Internet settings for server modules like Cloud connectivity, License Synchronization, View License History, Sending Email notifications and Messenger. This is very helpful in allowing the server modules to function in a secure work environment where default Internet connection is not allowed.

To provide Internet Settings, follow these steps:

1. Log on to the **Thirtyseven4 Endpoint Security web console**.
2. Go to **Admin Settings** > **Server** > **Internet Settings**.
3. To set the proxy setting for Internet, select **Enable Proxy Setting**.

The proxy settings details are activated.

4. In Proxy Server, type the server name.

5. In Port, type the port number.

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

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



The Internet Settings provided in Admin Settings will reflect in Update Manager Connection Settings.

Patch Management

Patch Management enables the centralized management for checking and installing the missing patches for the applications installed in your network. With this too, you can also automate checking and installation of the missing patches.

The Patch Management feature is applicable only for the clients with Microsoft Windows OS; does not support Mac operating system.

Installing Patch Server:

To install the patch server, follow these steps:

1. For 32-bit Windows OS, download the setup from the following link:
<http://updates.thirtyseven4.com/builds/2016/eps7.2/pmsetup32.msi>
For 64-bit Windows OS, download the setup from the following link:
<http://updates.thirtyseven4.com/builds/2016/eps7.2/pmsetup64.msi>
2. Launch the setup on the system in the network where you want to install the Thirtyseven4 patch server.
3. After the installation is complete, add Thirtyseven4 patch server through TSEPS console and then it becomes available to use.

Adding New Patch Server

To add new patch server, follow these steps:

1. Log on to Thirtyseven4 Endpoint Security Web console.
2. Go to **Admin Settings > Server > Patch Management**.
3. On the Patch Management page, click the **Add New Patch Server** tab.
4. In the Add New Patch Server section, enter Server Name.
5. If the Patch server is deployed in the network of local client, follow these steps:
 - i. In the **Server IP/Hostname** text box, type private IP address or host name of the Patch Server.
 - ii. In **Port**, type the port number. Default Port HTTP is 3698 SSL:6201.
 - iii. Ensure that the **Use SSL (Ensure Patch server supports SSL, if SSL is checked)** check box is selected. This check box is selected by default.
 - iv. In the TSEPS Details section, in the **TSEPS IP/Hostname** text box, provide private or public IP/Hostname of the TSEPS server. We recommend provide the Private IP/Hostname.

If the Patch server is deployed in the network of remote client, follow these steps:

- i. In the **Server IP/Hostname** text box, type public IP address or host name of the Patch Server.
 - ii. In **Port**, type the port number. Default Port HTTP is 3698 SSL:6201.
 - iii. Ensure that the **Use SSL (Ensure Patch server supports SSL, if SSL is checked)** check box is selected. This check box is selected by default.
6. Click **Add**.

Removing Patch Server

To remove the patch server, follow these steps:

1. Log on to Thirtyseven4 Endpoint Security Web console.
2. Go to **Admin Settings > Server > Patch Management**.

3. On the Patch Management page, click the **Add New Patch Server** tab.
4. Existing Patch Server Status appears. The status options are as follows:

Status	Description
Online	The patch server is online.
Offline	The patch server is offline.
Uninstalled	The patch server is being uninstalled.
Invalid	The patch server is added on TSEPS console. Then the same patch server is added on another TSEPS console. In this case, the status of the patch server in the first TSEPS will be shown as invalid.

5. You cannot remove a patch server, if it is applied to a policy. Select the Patch server that you want to remove and click the link **Remove** next to it.

A confirmation message appears.

6. Click **Yes** to remove the patch server.

Configuring Patch Server

Configure the port for Thirtyseven4 patch server to which TSEPS server and endpoints will communicate.

To configure the patch server, follow these steps:

1. Log on to Thirtyseven4 Endpoint Security Web console.
2. Go to **Admin Settings > Server > Patch Management**.
3. On the Patch Management page, click the **Configure Patch Server** tab.
4. Select the patch server from the list. Configuration section appears.
5. Select the **Configuration** tab and do the following:
 - i. The port number of the patch server appears. You can edit the port number.
 - ii. Select the check box **Use SSL (Select the check box if the patch server is configured with SSL)**.
 - iii. In the Automatic Download section, select the **Automatic download the detected missing patches if severity equal to or greater than:** check box.
 - iv. Select the severity level from the list. The severity options are:

Severity	Description
Critical	Vulnerability may allow code execution without user interaction.
Important	Vulnerability may result in compromise of the confidentiality, integrity, or availability of user data. The client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability.

Moderate	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.
Low	Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.
Unspecified	Vulnerability may result in random malfunctions.

6. Select the **Internet Settings** tab and do the following:

The details of the proxy server appears. By default, the Enable Proxy Settings check box is selected. You can clear the check box to disable the proxy settings.

- i. In the **Proxy Server** text box, the IP address of the proxy server appears. Edit the IP address if required.
- ii. In **Port** text box, the port number of the proxy server appears. Edit Port number if required.
- iii. Select the **Enable Authentication (if any)** check box to enable authentication.
- iv. In the **User name** and **Password** fields, type in your server credentials.

7. Select the **Patch Synchronization** tab and do the following:

- i. Previous patch synchronization status and last successful patch synchronization dates appear.
- ii. In the Configure Upstream Patch Server section, select the upstream patch server from the following options:

Upstream Patch Server	Description
Microsoft Patch server	The upstream patch server used is Microsoft patch server. This option is selected by default.
Organization Patch server (WSUS)	The upstream patch server used is Organization Patch server (WSUS - Windows Server Update Service). If you select this option, type in WSUS server URL.
Thirtyseven4 Patch server	The upstream patch server used is configured Thirtyseven4 Patch server. If you select this option, select the patch server from the list.

- iii. In the Configure Patch Synchronization section, select the **Enable Schedule Patch Synchronization** check box.
- iv. Select **Frequency** of patch synchronization, either Weekly or Monthly.
- v. Select **Weekday** from the list to run patch synchronization.
- vi. Select time to run patch synchronization by selecting hours and minutes in the **Start At** list.
- vii. Click **Filters..** to specify filters for patch synchronization. Windows Patch Synchronization Settings dialog appears.

- a. In the **Products** tab, select the Microsoft products for which you want to receive the patches. Select the folder to expand and then select.
 - b. Select the **Categories** tab. Select the type of patches to be synchronized.
 - c. Select the **Languages** tab. Select the languages for the patches by selection one of the following options:
 - Download patches in all languages
 - Download patches in below selected languages
 - d. Click **Apply** to apply the filters for patch synchronization. To restore the default settings, click the **Default**.
- viii. Click **Start** to run patch synchronization instantly.
 - ix. Click **Stop** to stop patch synchronization if it is running. A notification is sent to the patch management server.
8. Click **Apply** to apply the configuration settings.



Patch Management supports the following applications along with Microsoft applications,

- VideoLAN Player
- Adobe Acrobat
- Adobe Flash Player
- Adobe Reader
- puTTY
- Notepad++
- Oracle Corp.
- Java
- 7-zip compression Tool
- Mozilla Thunderbird
- Firefox

General

This feature helps you configure the settings about when the running session should time out. The session is timed out if the current session is inactive for the specific time.

To configure General, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Admin Settings > Server > General**.
3. From the Session time out period list, select the time period.
You can select either 20 minutes, 30 minutes, or 60 minutes.
4. Click **Apply**.

Multiserver Migration Period

Multiserver Migration Period feature allows you to install a higher version of TSEPS without uninstalling the previous one for a certain time, with this you can easily migrate the existing clients to a higher version. You can select the time period according to your schedule ranging from 30 to 90 days. Follow the given steps to use the feature:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Admin Settings > Server > General**.
3. In the Multiserver Duration list, select the number of days.
4. Click **Apply**.



- This option will only be available on the higher version installed in case of Multi-server installation.
- By default 60 days option is selected.

Clients

This section includes the following.

Client Installation

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

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

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to **Admin Settings > Clients > Client Installation**.
The Client Installation page appears.
3. To configure the client installation path, type the installation path in the **Please Specify Client Installation Path** text box.
4. From the Scan and Report section you can select following options to start the scan when SEPS gets installed:
 - Vulnerabilities: To configure the vulnerability scan of the client endpoint and send the report to SEPS server after successful installation of SEPS, you can select this check box.
 - All installed applications: To configure the scan of all the installed applications on a client endpoint after successful installation of SEPS, you can select this check box. The scan report is sent to the SEPS server. This option is selected by default.
5. To apply the setting, click **Apply**.



- The features are not available in the clients with Mac operating systems.

Inactive Client Settings

When you uninstall the Thirtyseven4 client from an endpoint, the program automatically notifies the server. When the server receives this information, it removes the client icon in the computer tree subsequently.

However, if the client is removed using other methods, such as you reformat the computer hard drive or delete the client files manually, Thirtyseven4 Endpoint Security will display the client as inactive. If a user unloads or disables the client for an extended period, the server also displays the client as inactive.

To protect the display of active clients, you can configure Thirtyseven4 Endpoint Security to remove inactive clients from the computer protection list.



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

To remove inactive clients, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. Go to Admin Settings > **Clients**.
The Client Installation page appears.
3. Under Inactive Client Settings, select the **Enable automatic removal of inactive clients** check box.
4. In the Remove a client if inactive for list, select number of days after which Thirtyseven4 Endpoint Security considers a Client is inactive.
5. To apply the setting, click **Apply**.

Asset Management

This feature helps in enabling collection of various information about endpoints such as, system information, hardware information, software installed, and updates installed.

You can enable the Asset Management reporting by the following procedure.

1. Log on to the **Thirtyseven4 Endpoint Security web console**.
2. Go to **Admin Settings > Clients**.
3. Select the **Enable Asset Management** check box.
4. Click **Apply**

Roaming Clients

Roaming service allows interacting with the TSEPS server via cloud when the clients are outside the organizational network. This allows the administrator to apply policies, initialize Tune-up, and scans like application control scan, vulnerability scan, and virus scan remotely from the TSEPS Server.

The clients can update their status (This will be displayed as Roaming on the Client status tab and Dashboard by default as the client goes roaming), download the latest configuration, and send client reports.

TSEPS will communicate with the cloud based roaming service using the Proxy settings configured using the internet settings tab, in case these settings are not available, TSEPS will use a direct connection.

You can enable the roaming service by the following procedure:

1. Log on to the **Thirtyseven4 Endpoint Security web console**.
2. Click **Admin Settings > Clients**.
3. Select **Roaming Clients**.
4. Click the **Connect to cloud platform**.

Connection Process Complete page is displayed.

5. Click **Ok**.
6. Check the **Enable Roaming Service** check box.
7. Select the Roaming mode for the clients:

- Automatic

In this mode, every TSEPS client can connect to Roaming Service automatically as it is out of the organizational network.

- Manual

In this mode, only selected clients can connect to Roaming Service. Selecting this mode enables you to select the specific clients, as follows:

- i. Click the **Select clients**.
- ii. To use this service, select the clients in your network and enable them to use this service.
- iii. Click **Ok**.

8. Click **Apply**

Reinstallation

In case of Reinstallation with the same product key, you need to activate the Roaming Clients as mentioned below:

1. Log on to the **Thirtyseven4 Endpoint Security web console**.
2. Go to **Admin Settings > Clients > Roaming Clients**.
3. Click Connect to cloud platform.
Connection Process Complete page is displayed.
4. Click OK.
5. Select the email address where you want to receive the OTP.

6. Click **Next**.
7. Check the given email address and click **Confirm** to receive the OTP.
8. Enter the OTP as received in the email.
9. If you have not received any mail, click **Regenerate OTP** to generate it again.
10. The connection process is complete. Click **Ok** to proceed.
11. Select **Enable Roaming Service** and **Roaming mode**.



- Roaming Clients feature is only supported for Windows and Mac operating systems.
- An internet connection is required for using this service.

Data Loss Prevention (DLP)

In this section, you can see the count of DLP licenses purchased and DLP licenses utilized. You can enable or disable the DLP Pack for any endpoints.

The page displays the following information,

- Total number of DLP licenses entitled (purchased)
- Number of DLP licenses utilized

Enabling DLP feature

To enable the DLP feature, follow these steps:

1. Log in to Thirtyseven4 EPS web console.
2. Go to **Admin Settings > Clients > Data Loss Prevention**.

A list is displayed with all the endpoints for which the DLP feature is enabled.

3. Click **Add**.

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

4. Under TSEPS Console, select a group.

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

5. Select an endpoint and then click **OK**.

The DLP feature is enabled for the selected endpoints.

You can also remove the endpoint, if you prefer.

Fields	Description
Search	Helps you search the endpoint by name.
CSV	Helps you save the list in csv format.
Add	Helps you add the endpoint to enable DLP for that endpoint.

Remove	Helps you remove the endpoint.
--------	--------------------------------



If the TSEPS client is removed from the client list, it will be removed from the DLP availed list also.

Chapter 13. Update Manager

Update Manager is a tool integrated with Thirtyseven4 Endpoint Security. It 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. All the Thirtyseven4 Endpoint Security clients fetch the updates from this centralized location. It also provides the facility of automatically updating Thirtyseven4 Endpoint Security for enhancements or bug fixes. Update Manager integrated with Thirtyseven4 Endpoint Security includes all the features that are available in the Update Manager application. Any change in settings made here will reflect in the Update Manager application.

Viewing Update Manager Status

Use this feature to view information of all types of updates downloaded by Update Manager. The console displays the Version, Service Pack, and the date of the associated Virus Database.

Additionally, the console also provides the following details:

Fields	Description
Endpoint Name	Displays the name of the endpoint where Update Manager is installed.
IP Address	Displays the IP address of the endpoint where Update Manager is installed.
Status	Provides the information about Update Manager, whether it is online or offline.
Update Manager URL	Provides the Update Manager URL to download the updates. This URL can be used by the alternate Update Manager, client, and other TSEPS Update Manager.

The two buttons available under Update Manager Status are:

Buttons	Description
Update Now	Click this button to send a Notification from Thirtyseven4 Endpoint Security to the Update Manager to start downloading the updates. This process is in the background and will not be visible to the user. Click Back to go to the Status page.
Rollback	<p>Click this button to take the Update Manager back to the previous update state.</p> <p>Note: This feature will work only if Always take backup before downloading new update option is selected in the settings of the Update Manager. The steps for performing Rollback are as follows:</p> <ul style="list-style-type: none">Click the Rollback button. A pop-up window opens. The Thirtyseven4 product updates that will be affected by the rollback are displayed.

	<ul style="list-style-type: none"> To begin the Rollback process, click Rollback.
--	---

Update Manager Settings

The following are the features available under Update Manager Settings:

Features	Description
Enable Automatic Updates	Select this box 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.
Always take backup before downloading new update	Select this box to enable and 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.
Delete report after	Select this box to enable deletion of reports automatically after the time you specify. This feature is enabled by default and the default time is 10 days.
Download the Thirtyseven4 Endpoint Security Service Pack	To take the updates for Thirtyseven4 Endpoint Security service pack, select Download Endpoint Security Service Pack check box. This feature is enabled by default.
Select the updates you want to download.	A list of TSEPS products appear. By default, all the products are selected. Verify which updates should be downloaded for your Endpoint security.
Restrict download speed (kbps)	Select the Restrict download speed (kbps) check box if you want to restrict the update download speed. Enter the speed in the text box. You can enter speed limit in the range of 64 kbps to 8192 kbps.

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

Update Manager Schedule

This feature helps you define the update schedules for the Update Manager at a certain frequency.

To configure Update Manager Schedule, follow these steps:

1. Log in to Thirtyseven4 EPS 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 **Update Manager Settings** tab.
4. Click the **Settings** button available next to Enable automatic updates.

The Update Manager Scheduler dialog appears.

5. Select the **Custom** option and configure the following options:

- i. In **Frequency**, select either the Daily or Weekly option.

If you select the **Weekly** option, select the weekday from the list.

- ii. In **Start At**, set time in hours and minutes.
 - iii. If you want to repeat the update of the Update Manager, select the **Repeat Update** check box and set the frequency in days to repeat the scan.
6. Click **Apply**.

Alternate Update Managers

In case of large network, you can deploy multiple Update Managers on different servers. This helps in load balancing and you can configure Clients in Client Settings to take the updates from these locations. You can view the details, add, edit or delete the Alternate Update Managers.

Recommendation

For remote clients, install the Alternate Update Manager in the network where the remote clients are deployed.

Adding New Alternate Update Manager

To add a new Alternate Update Manager in the TSEPS server, follow these steps:

1. Log on to the 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 Managers** tab.

A list of all Update Managers appears.

4. Click **Add** to create new Alternate Update Manager.
5. A list of endpoints where the Alternate Update Manager is installed on TSEPS clients appears.

Select the endpoint from the list to create Alternate Update Manager on that endpoint.

6. In the **Update Manager Name** text box, type the name.
7. In the **Update Manager Site** text box, type the URL of the Alternate Update Manager.
8. To save your settings, click **Add**.

Viewing details of Alternate Update Managers

To view details of Alternate Update Managers, follow these steps:

1. Log on to the 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.

A list of all Update Managers appears.

Update Manager

- Click the **Settings** link next to the Alternate Update Manager to view the status and settings of the Alternate Update Manager.
- The Alternate Update Managers Details screen appears. Click the **Status** tab to view the status with the following details:

Fields	Description
Update Manager Name	Displays the name of the Alternate Update Manager.
Endpoint Name	Displays the name of the endpoint where Alternate Update Manager is installed.
IP Address	Displays the IP address of the endpoint where Alternate Update Manager is installed.
Status	Provides the information about Alternate Update Manager, whether it is online or offline.
Update Manager URL	Provides the Update Manager URL to download the updates. This URL can be used by the alternate Update Manager, client, and other TSEPS Update Manager.

Also the list of the products installed with the details (Product Name, Version, Service pack and Virus Database Date) appears. The two buttons available under Update Manager Status are:

Buttons	Description
Update Now	Click this button to send a Notification from Thirtyseven4 Endpoint Security to the Update Manager to start downloading the updates. This process is in the background and will not be visible to the user. Click Back to go to the Status page.
Rollback	<p>Click this button to take the Update Manager back to the previous update state.</p> <p>Note: This feature will work only if Always take backup before downloading new update option is selected in the settings of the Update Manager. The steps for performing Rollback are as follows:</p> <ul style="list-style-type: none">Click the Rollback button. A pop-up window opens. The Thirtyseven4 product updates that will be affected by the rollback are displayed.To begin the Rollback process, click Rollback.

- Click the **Settings** tab to view the status with the following details:

The following are the features available under Alternate Update Manager Settings:

Features	Description
Enable Automatic Updates	Select this box 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.
Always take backup before downloading new update	Select this check box to enable and 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.

Update Manager

Delete report after	Select this check box to enable deletion of reports automatically after the time you specify. This feature is enabled by default and the default time is 10 days.
Download the Thirtyseven4 Endpoint Security Service Pack	To take the updates for Thirtyseven4 Endpoint Security service pack, select Download Endpoint Security Service Pack check box. This feature is enabled by default.
Select the updates you want to download.	A list of TSEPS products appear. By default, all the products are selected. Verify which updates should be downloaded for your Endpoint security.
Restrict download speed (kbps)	Select the Restrict download speed (kbps) check box if you want to restrict the update download speed. Enter the speed in the text box. You can enter speed limit in the range of 64 kbps to 8192 kbps.

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

Modifying Existing Alternate Update Manager details

To modify the details of an existing Alternate Update Manager, follow these steps:

1. Log on to the 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.
A list of all Update Managers appears.
4. Click the **Edit** link next to the Alternate Update Manager that you want to edit.
The Edit Alternate Update Manager dialog appears.
5. Modify the **Update Manager Name** and/or **Update Manager Site**.
6. To save you settings, click **Update**.

Alternate Update Manager Schedule

This feature helps you define the update schedules for the Alternate Update Manager at a certain frequency.

To configure Alternate Update Manager Schedule, follow these steps:

1. Log in to Thirtyseven4 EPS 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.
A list of all the Update Managers appears.
4. Click the **Settings** link available next to the Alternate Update Manager to view the status and settings of the Alternate Update Manager.
The Alternate Update Mangers Details screen appears.

Update Manager

5. Click the **Settings** tab.
6. Click the **Settings** button available next to Enable automatic updates.
The Update Manager Scheduler dialog appears.
7. Select the **Custom** option and configure the following options:
 - i. In **Frequency**, select either the Daily or Weekly option.
If you select **Weekly** option, select the weekday from the list.
 - ii. In **Start At**, set time in hours and minutes.
 - iii. If you want to repeat update of the Update Manager, select the **Repeat Update** check box and set the frequency in days to repeat the scan.
8. Click **Apply**.

Deleting Alternate Update Manager

To delete an existing Alternate Update Manager, follow these steps:

1. Log on to the 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.
A list of all Update Managers appears.
4. Select and then click **Delete** to delete the Alternate Update Manager.
A confirmation message appears. If you delete the update manager.
5. To delete the Alternate Update Manager, click **Yes**.

Chapter 14. License Manager

This feature allows you to manage the Thirtyseven4 Endpoint Security licenses. You can check the status of your Thirtyseven4 Endpoint Security license and update license information. You can place an order to renew your license, add new licenses to your existing setup, or buy additional features packs.

Status

This feature helps you check the current status of your license information. To check the status of your license, follow these steps:

1. Log on to the 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:

Title	Description
Company Name	Displays the name of the company to which Thirtyseven4 Endpoint Security is registered.
Product Name	Displays the product name. Example: Endpoint Security – Total.
Product Key	Displays the Product Key of Thirtyseven4 Endpoint Security.
Product Type	Displays the product type. Example: Regular.
Installation Number	Displays the installation number.
License valid till	Displays expiry date of the Thirtyseven4 Endpoint Security license.
Number of licenses utilized	Displays number of licenses utilized till date.
Number of licenses remaining	Displays number of licenses remaining.
Maximum number of licenses entitled	Displays total number of licenses purchased.
Maximum number of DLP licenses entitled	Displays total number of DLP licenses entitled. This will be visible only when the DLP feature is subscribed.

Update License Information

This feature is useful to synchronize your existing license information with Thirtyseven4 Activation Server. You can update your license information whenever required.

This is helpful in updating the following license information:

- License expiry date: If you have renewed the license but the expiry date is not updated or displays the old expiry date.
- Email ID: If there is any change in email IDs provided at the time of activation but has not reflected in the account.
- Feature changes or edition changes are synchronized with activation server.

If you want to renew your existing license and you do not know how to renew it or are facing any problem during renewal, you can call the Thirtyseven4 Support team and provide your Product Key.

View license history

You can view the details of your license purchase history if you click the License History button. On the License History page, the product details are displayed. Also the following information is displayed

- Date & Time: The time and date when the transaction was carried out.
- Activity: The type of purchase, such as license activation, pack addition, license renewal, license addition, and reactivation of license.
- Details: Relevant details of the transaction, such as type, number of licenses added, type of feature pack added or removed, and validity of the license purchased.

License Order Form

This feature helps you create a license order form for an additional license, renewal of your existing license, or edition upgrade. This is an offline activity and helps to create the license order.

After generating an order form, take out its print, contact a vendor or dealer, and submit it. You can also send an email with the license order form to the Thirtyseven4 sales team. We will contact you for further process.

To create a license order form, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. On the Home page, click the **View License** tab.
3. On the License Manager page, click the **License Order Form** tab.
4. To create a License Order form, select one of the following:
 - Renew my license: Helps you renew your current license.
 - Add license for new endpoints: Helps you buy additional licenses.
 - Edition Upgrade/Buy additional feature: Helps you upgrade the edition or buy additional features packs. as per the following table:

TSEPS Edition	Upgrade Pack
SME	Business/Total
Business	Total

5. Click **Place an Order**.

An order is created and an automated Email is sent to the Thirtyseven4 branch sales representative to process your order.

Renew my license

If you select the **Renew My License** option, you are redirected to the online portal of Thirtyseven4 where you can place an order for your license renewal. As you visit the portal, your license details are displayed.

On the Thirtyseven4 online portal, do the following:

1. In the Product Details section, verify your product license details. You can change Company Email Address, Admin Email Address and Phone Number if required.
2. In the renewal order section, select **Duration** for renewal.
3. Select **Number of the endpoints** (licenses) to renew for the systems.
4. To add the DLP Pack, select the DLP Pack check box. If you have the DLP pack subscription, you can assign the number of the endpoints to the DLP pack.
5. Select the number of endpoints to assign the DLP pack.
6. Click **Next**.

A summary of the license renewal order is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the Back button and make the required changes.

7. Type the email IDs to whom you want to send the order.
8. Click **Place a Request**.

Your license renewal request number is generated. Save this number as you will need to quote this number in all communications related to license renewal.

9. Click **Finish**.

Add license for new endpoints

If you select the **Add license for new endpoints** option, you are redirected to the online portal of Thirtyseven4 where you can place an order for additional licenses for endpoints. As you visit the portal, your license details are displayed.

On the Thirtyseven4 online portal, do the following:

1. In the Product Details section, verify your product **license details**. You can change Company Email Address, Admin Email Address and Phone Number if required.
2. Select the number of endpoints for which you want the additional licenses.

3. If you have the DLP pack subscription, you can assign the number of the endpoints to the DLP pack.

4. Click **Next**.

A summary of the additional license order is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the Back button and make the required changes.

5. Enter email IDs to whom you want to send the order.

6. Click **Place a Request**.

Your license addition request number is generated. Save this number as you will need to quote this number in all communications related to additional license order.

7. Click **Finish**.

Buy additional feature

If you select the **Buy additional feature** option, you are redirected to the online portal of Thirtyseven4 where you can place an order for a license for additional features. As you visit the portal, your license details are displayed.

On the Thirtyseven4 online portal, do the following:

1. Under Product Details, verify your product license details. You can change Company Email Address, Admin Email Address and Phone Number if required.
2. In the **Select the upgrade pack from the following:** section, select one of the following:
 - Business
 - Total

3. Select the **DLP pack** (Includes Data Loss Prevention) check box.

4. Select the number of endpoints to assign the DLP pack.

5. Click **Next**.

A summary of the order for feature packs is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the Back button and make the required changes.

6. Enter email IDs to whom you want to send the order.

7. Click Place a Request.

Your license request number for new feature packs is generated. Save this number as you will need to quote this number in all communications related to new feature packs.

8. Click **Finish**.

Edition Upgrade

If you select the Upgrade License option, you are redirected to the online portal of Thirtyseven4 where you can place an order for edition upgrade. As you visit the portal, your license details are displayed.

On the Thirtyseven4 online portal, do the following:

1. In the Product Details section, verify your product license details. You can change Company Email Address, Admin Email Address and Phone Number if required.
2. In the **Select the upgrade pack from the following:** section, select one of the following:
 - Business
 - Total
3. You can also select add-on feature pack. Select the **DLP Pack** check box.
4. Select the number of the endpoints to assign the DLP pack.
5. Click **Next**.

A summary of the order for upgrade packs is displayed. Verify it carefully as your order will be processed according to your preference. If you want to modify your order, you can go to the previous page by clicking the Back button and make the required changes.

6. Verify email IDs to whom you want to send the order.
7. Click **Place a Request**.

Your license request number for new upgrade packs is generated. Save this number as you will need to quote this number in all communications related to new upgrade packs.

Chapter 15. **Patch Management**

Patch Management (PM) enables the centralized management for checking and installing the missing patches for the applications installed in your network. With this you can also automate checking and installation of the missing patches.

Workflow of Patch Management

1. Install the Patch Management Server
2. Add Patch Management Server
3. Configure the Patch Management Server
4. Scan for missing patches
5. Select the missing patches and install the patches
6. Generate report of the installed missing patches

The procedure of installation is given below. Other steps of Patch Management are described as per occurrence on the console.

System requirements for Patch Management server

System requirements for Patch Management server are same as system requirements for Thirtyseven4 Endpoint security server. For more information, see System requirements for TSEPS server.

- For more than 25 clients, we recommend to install Patch Management server on the Windows Server operating system.
- Installation of Patch Management server is not supported on Microsoft Windows XP (32-bit) system.

The PM client is supported on Microsoft Windows XP (32-bit) system.

Recommendation

For the remote clients, install the Patch Server in the network where the remote clients are deployed. The private IP of the Patch server should be natted to public IP.

Installing Patch Management server on Windows Operating System

1. To begin installation of Patch Management server, follow these steps:

For 32-bit Windows OS, download the setup from the following link:

<http://updates.thirtyseven4.com/builds/2016/eps7.2/pmsetup32.msi>

Patch Management

For 64-bit Windows OS, download the setup from the following link:

<http://updates.thirtyseven4.com/builds/2016/eps7.2/pmsetup64.msi>

2. Launch the setup on machine within the network where you want to install the Thirtyseven4 patch server.

3. On the Patch Management Server Setup Wizard, click **Next**.

The license agreement appears. Read the License Agreement carefully.

4. Select the **I Agree** check box to accept the license agreement and then click Next.
5. Click **Browse** if you want to install Patch Management server on a different location. To proceed with the installation default path, click **Next**.
6. The Patch Database Settings screen appears. The patch content storage folder path appears. Click **Browse** if you want to change the patch content storage path.
7. Select the **Import Patch Server Data** check box if you want to change the default location. Click **Browse** to locate the path.

If TSEPS 7.0 patch server database backup is already exported, you can import the database in the TSEPS 7.2 patch server.

8. Click **Next**.

9. To enable and configure proxy settings, do the following:

- Select the **Enable Proxy Settings** check box.
- In the Proxy Server text box, type the IP address of the proxy server or domain name (For example, proxy.yourcompany.com).
- In **Port** text box, type the port number of the proxy server (For example: 80).
- Select the **Enable Authentication (If any)** check box.
- In the **User name** and **Password** fields, type in your server credentials.
- Click **Next**.

10. In the Upstream Patch Server screen, select one of the following:

- Microsoft: The upstream patch server used is Microsoft patch server. This option is selected by default.
- Organization Patch server (WSUS): The upstream patch server used is Organization Patch server (WSUS - Windows Server Update Service). If you select this option, type in WSUS server URL.

11. Click **Next**.

12. In the Website Configuration page, do the following:

- In the Server Configuration section, select one of the following:
 - Full Computer Name: Provide the computer name to configure the website
 - IP address: Provide the IP address of the target server. However, selecting IP address is not recommended if your network is configured using DHCP.
- In the **HTTP Port** text box, type a port number to use as the server listening port.

Patch Management

- **Enable Secure Socket Layer** check box is selected by default. Type the SSL port number. This port number will serve as a listening port for the server.
- Click **Next**.

13. On confirmation prompt, click **Yes**.

14. The installation summary screen appears. You can change your settings if required by clicking **Back**.

Click **Install**. The installation starts.

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

If installation / uninstallation is failed, then only the View installation log check box is displayed. To view the log, select the View installation log check box.

16. After the installation is complete, add Thirtyseven4 patch server through TSEPS console and then it becomes available to use.

The Patch Management feature is applicable only for the clients with Microsoft Windows OS; does not support Mac operating systems.

Recommendation for the remote clients

For the remote clients, install the Patch Server in the network where the remote clients are deployed. The private IP of the Patch server should be natted to public IP.

Back up the patch server data

You can back up the patch database and patch content of the patch server.

To back up the patch Server data, follow these steps:

1. Manually take backup of all the files and folders present in the <installation directory>/Thirtyseven4 patch management/patch server/content folder.
2. Select **Start > Programs > Thirtyseven4 Patch server Data Backup**. The Backup wizard starts.
3. Click **Browse** to specify the path where you want to back up patch database.
4. Click **Backup**.

The database file, pmdb.exp is generated. This file can be used to restore patch server data base.

Offline Patch Synchronizer

You can create an offline Patch Repository. Before repository creation, the Thirtyseven4 patch server must be synchronized for the patches of all required applications.

With the Thirtyseven4 offline Patch synchronizer wizard, you can do the following:

- 1) Creation of an offline patch repository from the Thirtyseven4 Patch Server.

2) Synchronization of the Thirtyseven4 patch server from the Offline Patch Repository.

This wizard creates an offline Patch Repository by importing patch server data from the Thirtyseven4 patch server.

An internet connection is required to download the patch contents if the patch contents are not available on the Thirtyseven4 Patch server.

To run the Thirtyseven4 offline Patch synchronizer wizard, follow these steps:

1. Select **Start > Programs > Thirtyseven4 offline Patch synchronizer**. The wizard starts.
2. Select one of the following,

- Create offline Patch Repository
- Synchronize from offline Patch Repository

3. If you select the option, Create offline Patch Repository, click Browse to specify the path where you want to create an offline Patch Repository.

If you select the option, **Synchronize from offline Patch Repository**, click **Browse** to specify the path which will be used to synchronize the Thirtyseven4 patch server.

4. Click **Finish**.

This wizard takes longer time for completion, when run for the first time, as per the patch server data size.

Use the same location next time to create the offline Patch Repository to add new patch server data. No need to create a new repository for the whole patch server data.

Patch Server Control Panel

You can view the status of patch management services with the help of Patch Server Control Panel. This view is used for troubleshooting purpose. To ensure that all the services are in running state for smooth functioning of the patch management server. You can also delete patch metadata and its content which are superseded or of older version.

To access the Patch Server Control Panel, follow these steps:

1. Select **Start > Programs > Patch Server Control panel**. The control panel opens.
2. In the Services section, you can see the current state of the Patch Management services.
3. Click **Start** to start the Patch Management services and all the dependent services. Click **Stop** when you want to stop the services.
4. Click **View Details** to view the status of the following patch management services,
 - AppPool - TSEPS Patch Scan 2.0
 - AppPool - TSEPS Patch Server 2.0
 - Website - TSEPS Patch Mgt 2.0
 - Service - MySQL - SQM20

Patch Management

- Service – sqpmSvc
5. In the Cleanup section, Click **Start** to delete patch metadata and its content which are obsolete. Click **Stop** when you want to stop the cleanup.

Uninstalling patch server

If you need to uninstall the patch server, follow these steps:

1. Go to **Start > Programs > Uninstall patch server**.
The uninstaller wizard starts.
2. Complete the wizard to uninstall the patch server.

Chapter 16. Technical Support

Thirtyseven4 provides extensive technical support for the registered users. It is recommended that you have all the necessary details with you during the call to receive efficient support from the Thirtyseven4 support executives.

Support

The Support option includes FAQ (Frequently Asked Questions) where you can find answers to the most frequently asked questions, options to submit your queries, send emails about your queries, or call us directly.

To access the Support options, follow these steps:

1. Log on to the Thirtyseven4 Endpoint Security web console.
2. On the top right on the Thirtyseven4 Endpoint Security Dashboard, click the **Support** button.
3. Support includes the following options:

Web Support

To view the frequently asked questions, click the **Visit FAQ** button or click the Visit Forums button to share tips, solutions, and to submit your queries.

Email Support

Email your query to support@thirtyseven4.com. Our Support team will respond to your query at the earliest.

Live Chat Support

This feature allows you to chat with the Thirtyseven4 technical executives to get your issues resolved.

Phone Support

This feature helps you to call the Thirtyseven4 technical experts for instant support.

Contact number for phone support: 1-877-374-7581

Contact time: Monday –Friday between 8.00 AM to 5.00 PM.

Remote Support

This support module helps us easily connect to your computer system remotely and assist you in resolving technical issues.

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

If the Product Key is Lost

Product Key serves as your identity to your Thirtyseven4 Endpoint Security product. If you lose the Product Key, please contact Thirtyseven4 Technical Support to get the Product Key. A nominal charge is levied for re-issuing the Product Key.

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.

Thirtyseven4 Support: <https://thirtyseven4.freshdesk.com/support/home>.

Web: www.thirtyseven4.com

Sales: sales@thirtyseven4.com.