Thirtyseven4 Tablet Security for Android

User Guide

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

Copyright Information

End-User License Agreement

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

1. License Grant and Restrictions

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

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

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

2. Fees

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

3. Ownership

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

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

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

4. Termination

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

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

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

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

5. Warranties and Indemnities

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

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

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

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

6. Controlling Law and Severability

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

7. Non-Binding Mediation

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

8. Limitation of Liability and Fees

COMPANY’S TOTAL LIABILITY, INCLUDING ANY DAMAGES, SHALL NOT EXCEED THE TOTAL AMOUNT USER PAID TO COMPANY. SHOULD COMPANY BE FORCED TO MEDIATE, ARBITRATE,

OR LITIGATE ANY DISPUTE AGAINST USER AND SHOULD COMPANY PREVAIL IN SUCH DISPUTE, USER SHALL REIMBURSE COMPANY FOR ALL OF ITS ATTORNEY FEES AND COSTS ASSOCIATED WITH THE ENTIRE DISPUTE, INCLUDING FEES OR COSTS INCURRED PRIOR TO ANY CLAIM BEING FILED AND ALL OF COMPANY'S COSTS, INCLUDING ATTORNEY'S FEES, ASSOCIATED WITH THE MEDIATION, ARBITRATION, OR LITIGATION.

9. Non-Waiver

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

10. Successors; Assigns

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

11. Use of Site Image

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

12. Complete Agreement

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

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

About the Document

This user guide covers all the information required to install and use Thirtyseven4 Tablet Security. We have followed certain set of conventions to prepare this guide. The table below lists the conventions used in 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.

Introducing Thirtyseven4 Tablet Security for Android

Thirtyseven4 Tablet Security is designed to protect Android tablet device. While using the device, users are at risk of exposing their devices and information in it to virus threats and the constant badger of unwanted messages (SMS) and calls. Thirtyseven4 Tablet Security has a host of features that protect the device effectively and enhance its performance.

Thirtyseven4 Tablet Security includes the following features:

Features	Description
Virus Protection	This feature provides continuous security and scans the device for viruses and unknown threats. This feature is always enabled and can be used even prior to activating Thirtyseven4 Tablet Security.
Call and SMS Block	This feature blocks calls from all non-contact numbers or a configured blacklist of specific contact numbers. As well as, blocks SMS from contacts, non-contacts, non-numeric senders, and blacklist.
Anti-Theft	This feature protects from the unauthorized access of the device and data stored in it. It helps remotely block the device, remotely wipe data, block device on SIM change, and trace the location if the device is lost or stolen.
Backup	This feature helps to take a backup of the personal information, such as contact numbers, text messages, calendar, and pictures on the Thirtyseven4 server and retrieve it whenever required.
Web Security	This feature blocks access to infected and fraudulent websites. It helps enable Parental Control to keep a tab on the online activities of children or other users.
Performance Monitor	This feature helps to check the functioning of the device, control power saver, speed up device efficacy, and view performance reports.
Network Monitor	This feature helps to manage all the networks available on the device and also keeps track of network usage.
Reports	Each of the application components has its own report that includes the information on the component operation (for example, information on a blocked SMS and Calls, scan report, updates etc.).

For more information, please visit http://www.thirtyseven4.com/.

Contents

Chapter 1. Getting Started

Thirtyseven4 Tablet Security is simple to install and easy to use. During installation, read each installation screen carefully and follow the instructions. Thirtyseven4 Tablet Security should be installed on an Android tablet device.

Prerequisites

Remember the following guidelines before installing Thirtyseven4 Tablet Security on the tablet device:

- A device with multiple anti-virus software apps installed may result in system malfunction.
- To avoid any issues, remove other anti-virus program before installing Thirtyseven4 Tablet Security.

System Requirements

Thirtyseven4 Tablet Security is designed for installation on tablet computers. Thirtyseven4 Tablet Security supports the following versions and resolutions of Android.

Supported Versions of Android

Thirtyseven4 Tablet Security supports the following versions of Android:

2.2, 2.3, 3.0, 4.0 and later.

Supported Resolutions of Android

Thirtyseven4 Tablet Security supports the following resolutions of Android:

- Small screen - 7 inches - 1024×600 , 800 x 480
- Large screen - 10 inches - 1280×800

Installing Thirtyseven4 Tablet Security

The latest Thirtyseven4 Tablet Security installer can be downloaded from the following website: http://www.thirtyseven4.com/downloads.html.

To download the installer, a 20-digit valid Product Key of Thirtyseven4 Tablet Security is required.

- For purchased copy, the Product Key is available in the Getting Started guide.
- For online users, the Product Key is sent to the registered email address.

To install Thirtyseven4 Tablet Security, follow these steps:

1. Go to the folder in the Android device where the Thirtyseven4 Tablet Security installer is placed, then tap on the **installer (.apk) file**.

   If the installer file is downloaded on PC, then copy the installer file on the Android device. From the device, tap **installer (.apk)** file to continue with installation.

2. In the **Install** screen, tap **Install**.
3. In the **Application installed** screen, the **Open** and **Done** buttons are displayed. Tap the **Done** button to finish installation.

   Thirtyseven4 icon is displayed in **All apps**.

4. To open the application, tap **Thirtyseven4 Tablet Security** in **All apps**.
5. In License Agreement screen, tap **I Agree** to go to the Activation screen.

Activating Thirtyseven4 Tablet Security

Once Thirtyseven4 Tablet Security is installed on the device, it is recommended to activate the product in order to use all the features and get technical support.

1. Go to **Thirtyseven4 Tablet Security**.
2. In **License Agreement** screen, tap **I Agree** to proceed to the Activation screen.
3. To activate the product, follow the instructions on the screen carefully.

To activate the product, users have to register the product. To know how to register Thirtyseven4 Tablet Security, refer Registering Thirtyseven4 Tablet Security section.

Uninstalling Thirtyseven4 Tablet Security

Uninstalling Thirtyseven4 Tablet Security exposes the device and its valuable data to virus threats. Hence it is advised to remove protection application only when formatting the device or installing it on another device.

NOTE: Before uninstalling Thirtyseven4 Tablet Security, it should be deactivated.

Deactivating Thirtyseven4 Tablet Security

To deactivate Thirtyseven4 Tablet Security, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. In the menu, tap **Help**.
3. Tap **Deactivation**.

4. In **When to deactivate Thirtyseven4 Tablet Security** screen, tap **Deactivate**.
5. On the confirmation screen for deactivation, tap **Yes**.

Uninstalling Thirtyseven4 Tablet Security

Before uninstalling Thirtyseven4 Tablet Security from the device, make sure the product is deactivated. This ensures that user can reinstall Thirtyseven4 Tablet Security later easily and successfully.

To know about how to deactivate the product, refer Deactivating Thirtyseven4 Tablet Security in the preceding section.

To uninstall Thirtyseven4 Tablet Security, follow these steps:

When Uninstallation Protection is enabled

Through Deactivation

NOTE: Thirtyseven4 recommends uninstallation through deactivation. This is applicable for licensed copy users only.

1. Go to **Thirtyseven4 Tablet Security**.
2. In the menu, tap **Help**.
3. Tap **Deactivation**.
4. In the **When to deactivate Thirtyseven4 Tablet Security** screen, tap the **Deactivate** button.
5. In the **Anti-Theft block** screen, tap **Unblock** and type the secret code and then tap **Go**.
6. In the deactivation confirmation screen, tap **Yes**.
7. Tap **OK**.
8. In uninstall application screen, tap **OK**.
9. Tap **OK**.

Through Device Settings

1. Go to the device settings.
2. Tap **Security**.
3. In the Security screen, tap **Device administrators**.
4. Clear the tick mark in front of Thirtyseven4 Tablet Security.
5. In the Device administrators screen, tap **Deactivate**.
6. In the Anti-Theft block screen, tap **Unblock** and type the secret code and then tap **Go**.

7. In the confirmation screen for deactivating the Device Admin, tap **OK**.
8. Now go to **Manage applications** in the device settings and tap **Thirtyseven4 Tablet Security**.
9. In the app info screen, tap **Uninstall**.
10. In the confirmation screen for uninstalling the application, tap **OK**.
11. To close the screen, tap **OK**.

When Uninstallation Protection is not enabled

Through Deactivation

NOTE: Thirtyseven4 recommends uninstallation through deactivation. This is applicable for licensed copy users only.

1. Go to **Thirtyseven4 Tablet Security**.
2. In the menu, tap **Help**.
3. Tap **Deactivation**.
4. In the **When to deactivate Thirtyseven4 Tablet Security** screen, tap the **Deactivation** button.
5. If Anti-Theft is configured, the Anti-Theft block screen appears. Tap **Unblock** and type the secret code and then tap **Go**.
6. The **When to deactivate Thirtyseven4 Tablet Security** screen appears, irrespective of the Anti-Theft is configured or it is not configured.
7. In the confirmation screen, tap **Yes**.
8. In the Deactivation confirmation screen, tap **OK**.
9. In the uninstall application screen, tap **OK**.
10. To close the screen, tap **OK**.

Through Device Settings

1. Go to the device settings.
2. Tap **Applications** and then tap **Manage applications**.
3. Tap **Thirtyseven4 Tablet Security**.
4. In the app info screen, tap **Uninstall**.
5. In the Anti-Theft block screen, tap **Unblock** and type the secret code and then tap **Go**.
6. In the confirmation screen to uninstall the application, tap **OK**.
7. To close the screen, tap **OK**.

Chapter 2. Registration, Reactivation, Renewal

Thirtyseven4 Tablet Security must be immediately registered after installation to activate the copy. Only the activated copy will receive the database updates and technical support whenever required. If the product is not regularly updated, it cannot protect the device against the latest threats.

Registering Thirtyseven4 Tablet Security

Thirtyseven4 Tablet Security is simple to register.

To register the product, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. In the License Agreement screen, tap **I Agree**.
3. In the Registration Type screen, tap **Activation**.
4. Enter the 20-digit valid product key in the **Enter Product Key** text box.
5. Enter relevant information in the **User Name**, **Mobile Number**, **Email Address**, and **Confirm Email Address** text boxes. Enter the mobile number only if the registration is done through Internet.
6. Tap **Submit**.

Reactivating Thirtyseven4 Tablet Security

Install and reactivate Thirtyseven4 Tablet Security on the device whenever required.

To reactivate Thirtyseven4 Tablet Security, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. In the License Agreement screen, tap **I Agree**.
3. In the Registration Type screen, tap **Activation**.
4. Enter the 20-digit valid product key in the **Enter Product Key** text box.
5. Enter the relevant information in the **User Name**, **Mobile Number**, **Email Address**, and **Confirm Email Address** text boxes.
6. Tap the **Submit** button.

Renewing Thirtyseven4 Tablet Security

Renewing the product before the validity date expires, protects it from unknown and malicious threats. It also gives the flexibility to use all the features and avail support.

To renew the Thirtyseven4 Tablet Security license, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. In the menu, tap **Help**.
3. Tap **About**, and then tap **Renew Now**.

Two options **Buy Renewal** and **Renew my License** appear. To buy a renewal or renew the license, follow the steps mentioned under respective options.

Buy Renewal

1. To buy renewal code online from a PC, tap **Renew Online**.
2. Contact the nearest dealer in the locality to buy a renewal code by tapping **Locate a Dealer**.
3. To get assistance in buying renewal code, contact the Thirtyseven4 Renewal Team by tapping **Call Us**.

Renew My License

If the renewal code is already purchased, proceed further to renew the license.

1. In the Renew Option screen, tap **Renew My License**.
2. Product Key is displayed in the text box.
3. Enter the renewal code.
4. If required, edit the mobile number and email ID.
5. Tap the **Submit** button.

Chapter 3. Using Thirtyseven4 Tablet Security Dashboard

The Thirtyseven4 Tablet Security Dashboard is divided into four sections; notification area, security status, main screen, and the menus.

Notification Area

Notification area displays the call or message received from a blocked number or virus detected.

Security Status

The security status is displayed on Dashboard. It gives information of various events such as virus protection is enabled or disabled and license expiry information. Dashboard displays security situation messages as mentioned in the table below.

Security Status	Message
Copy is not registered	Register Now!
Specific (30) days left for expiry	License period expires in 30 days! License period expires today!
License expired.	License period has expired. Renew Now!
Virus protection is ON	Your tablet is secure!
On Virus Protection disable	Your tablet is not secure! Virus protection is Off!
Not Updated since 7 days	Protection is out of date! Update Now!
Virus data base date is older than current date by 15 days	Protection is out of date! Update Now!

Thirtyseven4 Tablet Security Dashboard Features

Dashboard's main screen displays commonly used features of Thirtyseven4 Tablet Security and can be accessed directly. These features are as follows:

Features	Description
SMS Blocking	Blocks messages (SMS) from contacts, non-contacts, non-numeric senders, and blacklist.
Call Blocking	Blocks calls from all non-contact numbers or blacklist of specific contact numbers.
Anti-Theft	Protects the device and data stored in it from unauthorized access. Helps remotely block the device, remotely wipe data, block the device on SIM change, and trace device location.
Web Security	Helps to block infected and fraudulent websites that may harm or phish the confidential information. Also helps in setting Parental Control to help regulate the online activities of children or other users.
Virus Protection	Provides continuous protection and scans device for viruses and unknown threats.
Backup	Takes back up of valuable device data to Thirtyseven4 server. This data can be retrieved whenever required.
Performance	Checks the performance of the device, controls power saver, speeds up device performance, and helps in viewing the performance reports.
Network Monitor	Manages all the networks available on the device. It checks the current usage of all the networks and controls the usage.
Messenger	Provides updates about tablet protection, security alerts, or other important issues.
Scan Now	Helps scan the entire device or only memory cards.

Thirtyseven4 Tablet Security Menu

The Thirtyseven4 Tablet Security menu includes all the features. If the feature is not available on Dashboard, it can be found in the menu.

To access a feature under menu:

1. Go to **Thirtyseven4 Tablet Security.**
2. Tap the menu, next to the Thirtyseven4 Tablet Security icon.

Chapter 4. Using Thirtyseven4 Tablet Security

Thirtyseven4 Tablet Security with easy user-interface is designed to simplify the task of securing the device. Thirtyseven4 Tablet Security can be accessed from the Home Screen in any of the following ways:

- By selecting **menu > Apps >Thirtyseven4 Tablet Security**.
- By selecting **menu >Widgets > Thirtyseven4 Tablet Security**.
- By tapping **Thirtyseven4 Tablet Security Icon**.

There are number of smart features that helps to protect and manage the tablet device. These include:

Scan Now

With this feature, the device can be scanned whenever required. It includes the following scanning options:

- **Full Scan**: Includes scanning of the entire device.
- **Scan Memory Card**: Includes scanning of the memory card.

To initiate scanning of the device, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Scan Now**.
3. Select either **Full Scan** or **Scan Memory Card** as required to begin scanning.
4. Tap **View Details** when scan is complete to see the report if any threat is found.
5. In case virus is found in already installed applications, tap the **Resolve Now** button and select the application.
6. Choose either Skip or Uninstall option.
7. If virus is not found, the **No threats found** message is displayed.

NOTE: If manual scan is done, the device will be scanned for viruses irrespective whether Virus Protection is enabled or disabled through Virus Protection feature.

SMS Blocking

With SMS Blocking, all the unwanted messages (SMS) such as news, advertisements, marketing messages, offensive texts are blocked.

This feature also blocks messages from non-contact numbers, specific contact numbers, and non-numeric numbers. Configuring whitelist and blacklist, provides filtration for SMS blocking.

NOTE: The blacklist and the whitelist may include the contacts that are either available or not available in the phone directory.

To configure SMS Blocking, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **SMS Blocking**. Alternatively, select **menu > SMS Blocking**.

SMS Blocking Features

SMS Blocking includes the following features:

Blocked SMS

This feature displays a list of blocked messages received from blocked contact numbers. These messages can be read and moved to the message box. They can also be forwarded to any other contact or deleted if not required.

Settings

Settings helps to enable SMS scan, block spam messages, block SMS from contacts, non-contacts, and non-numeric senders. It enables **Show notifications of blocked SMS** whenever the user receives a message from the blocked contacts.

To configure Settings, follow these steps:

1. In the SMS Blocking menu, tap **Settings.**
2. To enable scanning of messages, turn **Enable SMS Scan** ON.
3. To block spam messages, turn **Block SMS Spam** ON.
4. To block messages from the contacts of phone directory, turn **Block SMS from Contacts** ON.
5. To block messages from the contacts that are not in the phone directory, turn **Block SMS from Non-Contacts** ON.
6. To block messages from non-numeric senders, turn **Block SMS from Non-Numeric Sender** ON.
7. To get the notification when a SMS is received from a blocked contact, turn **Show notifications of blocked SMS** ON.

Black List

This feature helps to create a blacklist of contacts. Messages from the blacklisted contacts will be blocked.

To create a blacklist of contacts, follow these steps:

1. In the SMS Blocking menu, tap **Black List**.
2. To add a contact, tap the plus sign (+).
3. In the Add contact to black list screen, type the contact number in the text box or add a contact from the phone directory by tapping the **Contact list** icon.
4. To block calls from the same contact, select the **Block Call from selected contacts**.
5. To save, tap the **Save** button.

Be sure that the contact entered in the blacklist does not exist in the whitelist.

White List

This feature helps to create a whitelist of contacts. Messages from the whitelisted contacts will be allowed. This provides privilege to receive messages from certain trusted contacts.

To create a blacklist of contacts, follow these steps:

1. In the SMS Blocking menu, tap **Black List**.
2. To add a contact, tap the plus sign (+).
3. In the Add contact to black list screen, type the contact number in the text box or add a contact from the phone directory by tapping **Contact list** icon.
4. To block calls from the same contact, select the **Block Call from selected contacts**.
5. To save, tap the **Save** button.

Be sure that the contact entered in the whitelist does not exist in the blacklist.

Spam Keywords List

This feature helps to create a list of spam keywords. It blocks the incoming SMS containing any of the keywords added to the list.

To create spam keyword list, follow these steps:

1. In the SMS Blocking menu, tap **Spam Keyword List**.
2. To add spam keywords, tap the plus sign (+).

3. In the Add keyword to Spam Keyword List screen, enter the valid spam keyword in the text box.
4. To save your spam keyword, tap the **Save** button.

Call Blocking

With Call Blocking, all unwanted calls such as sales calls, promotional calls, and other unnecessary calls are blocked.

This feature enables call block and blocks specific contacts and non-contact numbers that are added to the blacklist. The blacklist may include the contacts that are either available or not available in the phone directory.

To configure Call Blocking, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Call Blocking**. Alternatively, select **menu** > **Call Blocking**.

Call Blocking Features

Call Blocking includes the following features:

Blocked Calls

This feature displays a list of blocked calls received from blocked contact numbers. Users can check the blocked calls, remove them from the blacklist, and delete them if not required.

Settings

Settings enable call block and blocks calls received from non-contacts. Users can enable **Show notifications of blocked Calls** whenever a call is received from the blocked contact.

To configure Settings, follow these steps:

1. In the Call Blocking menu, tap **Settings**.
2. To enable call block, turn **Enable Call Block** ON.
3. To block calls from non-contacts, turn **Block Calls from non-contacts** ON.
4. To get notification on calls from blocked contact, turn **Show notifications of blocked Calls** ON.

Black List

This feature helps to create a blacklist of contacts. Calls from blacklisted contacts will be blocked.

To create a blacklist of contacts, follow these steps:

1. In the Call Blocking menu, tap **Black List**.
2. To add a contact, tap the plus sign (+).
3. In the Add contact to black list screen, type the contact in text box or add a contact from phone directory by tapping the **Contact list** icon.
4. To block SMS from the same contact, select **Block SMS from selected contacts**.
5. To save, tap the **Save** button.

Anti-Theft

The tablet gives a privilege of making a call, store important contacts, store confidential data, and access the Internet. The Anti-Theft feature protects the device data from unauthorized access when the device is lost or stolen. This feature blocks the device remotely, wipe the confidential data, block device on SIM change, and trace the device if lost or stolen.

The blocked tablet screen displays the owner comment with alternate contact number of the owner. On SIM change, a message to the authorized owner is sent to the alternate contact number. This helps to get back the device or trace its location.

To configure Anti-Theft, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Anti-Theft**. Alternatively, select **menu** > **Anti-Theft**.
3. In Enable Anti-Theft in just 3 steps screen, tap **Setup Anti-theft**.
4. In the Configure secret code screen, enter **Secret Code** and **Confirm Secret Code.**
5. Tap the **Next** button.
6. In Security Questions screen, choose two Security Questions. Enter appropriate answers to the selected questions. In case user forgets secret code, security questions will help reset the secret code.
7. Tap the **Next** button.
8. In the Alternate Contact screen, tap the **Contacts** button. In **Alternate Contact Number** text box enter alternate contact number or type a contact/non-contact number.
9. Under Uninstallation Protection section, select **Uninstallation Protection**.

   NOTE: This option makes the application more secure as no unauthorized users can remove the application from the device.
10. Tap the **Save** button.

11. Tap the **OK** button to finish the Anti-Theft setting or tap **View Demo** to see the blocked screen of the device. This demo is of ten seconds and disappears thereafter automatically.
12. If the Uninstallation Protection option is selected, the Device Administrators screen for Thirtyseven4 appears.
13. To secure the application uninstallation, tap **Activate** on the Device Administrators screen.
14. To disable Uninstallation Protection, tap the **Cancel** button.

NOTE: If the Uninstallation Protection option is not selected while configuring Anti-Theft, still the users can select this option later. To enable protection, go to the Anti-Theft setting screen and turn Uninstallation Protection ON.

The active SIM is taken as Trusted SIM. To know more about what Trusted SIMs are, see Trusted SIMs List in the following section.

- The alternate contact number (Contact Owner) is displayed on the blocked device screen with the owner comment. It helps to trace the lost or stolen device.
- If the SIM card of lost device is changed, instant message is sent on the configured alternate number. This message gives information about the new mobile number.
- If the Remote Data Wipe feature is used, all contacts, pre-selected folders, pictures, and SMS stored in the device are removed.
- Remotely lock the device or remotely wipe the data or trace device location by sending the following messages from any device to the lost device.
    - To remotely lock the device, send: BLOCK antitheft_secret_code (For example – BLOCK XXXXXXXXXX).
    - To remotely unblock the device, send: UNBLOCK antitheft_secret_code (For example – UNBLOCK XXXXXXXXXX).
    - To remotely wipe data, send: WIPE antitheft_secret_code (For example – WIPE XXXXXXXXXX).
    - To get device location, send: TRACE antitheft_secret_code (For example – TRACE XXXXXXXXXX).
    - To ring the device, send: RING antitheft_secret_code (For example – RING XXXXXXXXXX).

NOTE: 'XXXXXXXXXX' stands for the secret code that was set while configuring Anti-Theft.

Turning Uninstallation Protection ON

To make the Thirtyseven4 application more secure, add the application in the Device administrators. This will not allow any unauthorized person to uninstall the application from the device; however this is optional.

To turn Uninstallation Protection ON, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Anti-Theft**. Alternatively, on the **menu** > tap **Settings** > tap **Anti-Theft.**
3. Follow the steps from Step 3 to Step 8 as described in the Anti-Theft section.
4. Under Uninstallation Protection, select **Uninstallation Protection**.
5. Tap the **Save** button.
6. On the **Anti-Theft enabled successfully** message, tap **OK** to finish. Tap **View Demo** to see the blocked screen of the device. This demo is of ten seconds and it disappears thereafter automatically.
7. In the Device Administrator screen, tap **Activate**.

NOTE:

- If the Uninstallation Protection option is not selected while configuring Anti-Theft, still users can select this option later. To enable protection, go to the Anti-Theft setting screen and turn Uninstallation Protection ON.
- To uninstall Thirtyseven4 Tablet Security, first deselect the Uninstallation Protection.

Turning Uninstallation Protection OFF

The Uninstallation Protection can be turned off in two different ways.

Through Anti-Theft

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Anti-Theft** and then type the secret code.
3. Tap **Go**.
4. In the Anti-Theft Settings screen, turn **Uninstallation Protection** OFF.
5. In confirmation screen, tap **OK**.

Through Device Settings

1. Go to the device settings.
2. Select **Security > Device administrators**.
3. Clear the **Thirtyseven4 Tablet Security** option.
4. In the confirmation screen, tap **Deactivate**.
5. In the Anti-Theft Block screen, tap **Unblock.**
6. In the Unblock Device screen, type the secret code.

7. Tap **Go**.
8. In confirmation screen, tap **OK**.

Trusted SIMs List

This feature is useful for users using dual-SIM device or multiple SIM cards. It helps to add or remove additional SIMs to the Trusted SIMs list. Thus, when SIM is changed, the device is not blocked.

Trusted SIMs list is a list of SIM cards that are considered reliable and safe. The device is not blocked if a SIM from the trusted list is being used. Fifty (50) SIM cards can be added to this list.

If Anti-Theft is configured and a new SIM card is detected, which is not included in the Trusted SIMs list on the device, the phone gets blocked. However, when Anti-Theft is enabled for the first time, the SIM card present in the device is taken as trusted SIM automatically.

To add SIMs to the Trusted SIMs list, restart the phone with a new SIM and add the SIM to the Trusted SIMs list when prompted.

Unblocking Your Device

If the device is locked by mistake or lost or the SIM is changed from lost device, a message **Tablet is blocked** is displayed on the device screen.

To unblock the device, follow these steps;

1. Tap **Unblock**.
2. Enter the secret code in the Secret Code text box that was set while configuring Anti-Theft.
3. Tap **Go**.

In case, the user forgets the Secret Code, still the device can be unblocked. Set new secret code in the following ways:

Unblock Using Forgot Code option

1. On the device screen, tap **Unblock**.
2. Tap **Forgot Code?**
3. Enter answers to the **Security Questions** that appear.
4. Tab **Submit**.
5. In the Change Secret Code screen, enter **New Secret Code** and **Confirm Secret Code**.
6. Tap the **Save** button.

Unblock using recovery code option

1. On the device screen, tap **Unblock**.
2. Tap **Unlock using recovery code**.
3. Tap the **link** that appears to obtain recovery code.
4. Enter the **Product Key** and **Email Address** that was used during activation.
5. A recovery code is sent to the registered email ID.
6. In the **Unblock Tablet** screen, enter the recovery code in the text box.
7. Tap the **Submit** button.
8. Enter a new secret code in the **Secret Code** and **Confirm Secret Code** text box.
9. Tap the **Next** button.
10. Select the questions and enter answers in the **Answers** text boxes.
11. Tap the **Save** button.

In case the user forgets the answers to security questions, still the device can be unblocked. Reset security questions in the following way:

Forgot Answers to Security Questions?

To unblock the device, follow these steps;

1. On the device screen, tap **Unblock**.
2. Tap **Forgot Code?**
3. Enter any invalid answers to the security questions. Tap the **Submit** button.
4. Tap **Forgot Answers?**
5. Tap the link that appears to obtain recovery code.
6. Enter the **Product Key** and **Email Address** that was registered during activation.
7. In the **Unblock Device** screen, enter the recovery code in the text box.
8. Tap the **Submit** button.
9. Enter a new secret code in the **Secret Code** and **Confirm Secret Code** text box.
10. Tap the **Next** button.
11. Choose **Questions** and enter the **Answers** to them.
12. Tap the **Save** button.

Web Security

With Web Security, block infected and fraudulent websites that may harm or phish the confidential information. The Parental Control option helps to regulate online activities of the children or other users.

NOTE: The Web Security feature supports only the default browser of Android and Google Chrome browser.

To configure Web Security, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Web Security**. Alternatively, select **menu > Web Security**.

Web Security Features

Web Security includes the following features:

Settings

Settings help to enable browsing protection and phishing protection.

To configure Settings, follow these steps:

1. In the Web Security menu, tap **Settings.**
2. To block access to the infected websites, turn **Browsing Protection** ON. By default this option is turned ON.
3. To block access to the fraudulent websites, turn **Phishing Protection** ON. By default this option is turned ON.

Parental Control

With Parental Control, parents can restrict categories of websites or block specific websites. They can also allow access to trusted sites, even from a blocked website category. For example, if the category of social networking sites is blocked, the Facebook will be accessible.

To configure Parental Control, follow these steps:

1. In the Web Security menu, tap **Parental Control**.
2. To enable Parental Control, turn **Parental Control** ON.

   NOTE: By default Parental Control and Exclude Websites option is enabled.
3. To block the categories of websites, select **Categories**. All the sites falling under a category will be blocked.

Exclude Websites

Exclude Websites option allows access to a specific website, even if that website falls in a category that was blocked. For example, if the Social Networking sites category is blocked, Facebook is accessible.

To configure Exclude Websites option, follow these steps:

1. In the Web Security menu, tap **Exclude Websites**.

   NOTE: The Excluded Websites list appears if websites are already entered, else a message appears. Exclude websites option is activated only if Parental Control is enabled.

2. To add a website, tap the plus sign (+).

   In Add URL to Exclude screen, enter the website URL and then tap the **Save** button.
   NOTE: Be sure that same URL is not entered that exists in the Restrict Websites list.

Restrict Websites

Restrict Websites option blocks access to the specific websites. This is also helpful when a website does not fall in a correct category or if the website category is restricted yet a certain website is accessible that needs to be blocked.

NOTE: This feature is available only with Android OS previous to version 4.0.

To configure Restrict Websites options, follow these steps:

1. In the Web Security menu, tap **Restrict Websites**.

   NOTE: The Restrict Websites list appears if websites are already entered, else a message appears.

2. To enable Restrict Websites, turn **Restrict access to specified websites** ON.
3. To add a website, tap the plus sign (+).
4. In Add URL to Block Access screen, enter the website URL and then click the **Save** button.
   NOTE: Be sure that the same URL is not entered in the existing Exclude Websites list.

Virus Protection

With Virus Protection, the device is monitored continuously for virus threats caused by an email attachment, Internet downloads, file transfer, file execution and so on. However, Virus Protection is turned ON by default to protect from any potential threats.

The virus protection features are as follows:

Features	Description
Scan Settings	Helps Repair, Delete, or Skip when virus is found.
Virus protection	Helps to enable or disable Virus Protection. It takes action such as Repair, Delete, or Skip when virus is found.
Advanced Protection	Helps secure the device from applications having security risks (PUA) and adware.
Quarantine	Helps delete the quarantined files after the configured schedule.
Exclusion	Helps exclude applications, files, or folders from Virus Scanning.

Configuring Scan Settings

With Scan Settings, set the actions required when a virus is detected.

To configure Scan Settings, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Virus Protection**. Alternatively, select **menu** > **Anti Virus** > **Virus Protection**.
3. In the Anti Virus screen, tap **Scan Settings**.
4. Select any one action, such as Repair, Delete, or Skip.

NOTE: The actions configured here will be performed automatically during the scanning.

Configuring Virus Protection

To configure Virus Protection, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Virus Protection**. Alternatively, select **menu** > **Anti Virus** > **Virus Protection**.
3. To enable Virus Protection, turn **Virus Protection** ON.
4. Select an action to be taken when a virus is found from the **Action to perform when a malware is found** list.
5. To get notification on when virus was found and action on it, turn **Display virus protection alert message** ON.

Configuring Advanced Protection

To configure Advanced Protection, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Virus Protection**. Alternatively, select **menu** > **Anti Virus** > **Virus Protection**.

3. In the Anti Virus screen, tap **Advanced Protection**.
4. Enable or disable either options;
   - Scan Application having security risks (PUA): Detects the applications that can harm the device.
   - Scan Adware: Check for any possible applications that are capable of displaying advertisements that consume the balance and Internet usage.

     NOTE: However, these options are turned on by default.

Configuring Quarantine

To configure Quarantine, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Virus Protection**. Alternatively, select **menu > Anti Virus > Virus Protection**.
3. In the Anti Virus screen, tap **Quarantine**.
4. Turn **Delete quarantined files** ON to enable this feature. However, this feature is enabled by default.

   NOTE: If Delete quarantine files is turned Off, the frequency option is disabled and frequency cannot be set.
5. Select the frequency to delete the quarantined files from the given options: After 7 days or After 30 days or After 45 days.

Configuring Exclusion

With Exclusion, exclude applications, files, and folders from scanning.

To configure Exclusion, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Virus Protection**. Alternatively, select **menu > Anti Virus > Virus Protection**.
3. In the Anti Virus screen, tap **Exclusion**. Two tabs **Excluded Apps** and **Excluded Files and Folders** are displayed.
4. To exclude applications, tap **Excluded Apps** and then do the following:
   - Tap the plus sign (+).
   - From the application list, select the applications to be excluded and tap the **Save** button.
5. To exclude files and folders, tap **Excluded Files and Folders** and then do the following:
   - Tap the plus sign (+).

- From the list of files and folders, select the files and folders to be excluded and tap the **Save** button.

Backup

With Backup, take back up of valuable data such as contact numbers, calendar, messages (SMS), and pictures. This data is saved in Thirtyseven4 server and can be retrieved whenever required.

To configure Backup, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Backup**. Alternatively, select **menu > Backup**.
3. To take the backup of the data, go to the Backup Settings feature and then select the data types under **Take backup to secure your important information**.
4. To take the backup automatically, turn **Automatic Backup** ON.
5. From the Backup Schedule list, select the time frequency for automatic backup, such as; After 7 days or After 30 days or After 45 days.

   NOTE: However, the Backup Schedule At every day is selected by default.

Using Data Backup

With Data Backup option users can restore the backup, delete the backup, and take the backup manually whenever required.

Once the Automatic Backup is turned ON, the data is stored automatically to the Thirtyseven4 server. Restore this data whenever required.

Taking Backup Manually

Take the back up of the data manually, irrespective whether Automatic Backup is turned ON or OFF.

To take the backup manually, follow these steps:

1. In the Backup menu, go either to **Backup Settings** or **Data Backup**.
2. Tap **Backup Now**.

NOTE: Backup is taken for the data types selected in the Backup Settings feature. If a new file is added to the existing files, then backup of the newly added file is taken. This is because; the existing files were backed up earlier.

Restore Backup

Restore the backup if the data is lost for any reason. Backup of the data can be restored from the last backup taken as configured in Backup Settings.

To restore the backup, follow these steps:

1. In the Backup menu, tap **Data Backup**.
2. To restore the data, tap **Restore Backup**.

Deleting Data

Delete the backup; if the data is obsolete. However, once the data is deleted, it cannot be retrieved.

To delete the data, follow these steps:

1. In the Backup menu, tap **Data Backup**.
2. To delete the backup, tap **Delete Backup**.

Performance

With Performance, check the functioning of the device, control power saver, speed up device performance, and view the performance reports.

To configure Performance, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Performance**. Alternatively, select **menu** > **Performance**.
3. In Summary, check the current performance of the device, settings for power saving mode, and all the applications running.

Safe List

The applications added to Safe List are not killed automatically.

To add applications to Safe List, follow these steps:

1. In the Performance menu, tap **Safe List**.
2. To add an application in Safe List, tap the plus sign (+).
3. In the Add to Safe List screen, select the applications to add to the Safe List.
4. To save your settings, tap the **Save** button.

Power Saving

This feature enables power saver and take steps to save power to increase the battery life.

To configure Power Saving, follow these steps:

1. In the Performance menu, tap **Power Saving**.
2. To enable Power Saving, turn **Enable Power Saving** ON.
3. To set a percentage for power saving, tap **Active power saving mode if battery is below**.

4. A slider appears. Adjust the percentage on the slider.
5. To set brightness when in power saving mode, tap **Set brightness of screen to**.
6. A slider appears. Adjust the percentage on the slider. It is ideal to set lower brightness in power saving mode.
7. Select any of the following options as required to save the power:
   - Select **Disable Wi-Fi in power saving mode**.
   - Select **Disable Bluetooth in power saving mode**.
   - Select **Disable Mobile Network in power saving mode**.
   - Select **Kill all running apps**.
   - Select **Kill apps from safe list also**.

Speed Up Device

This feature enhances the performance of the device by stopping the running apps and killing idle apps on a regular basis.

To configure Speed Up Device, follow these steps:

1. In the Performance menu, tap **Speed Up Device**.
2. To enable stopping of apps, turn **Enable apps kill on screen lock** ON.
3. Set frequency when to kill apps on screen lock in the **Kill apps on screen lock after** list.
4. To set stopping of apps, turn **Enable apps kill schedule** ON.
5. Select a frequency to kill running apps from **Frequency to kill running apps** list.

Reports

This feature generates reports on how many apps were killed and when. The reports can be viewed for the current and previous month.

To view reports, go to the Performance menu, and tap **Reports**.

Network Monitor

With Network Monitor, manage all the networks used on the device. Network Monitor checks the current usage of all the networks and controls the usage.

To configure Network Monitor, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. On Dashboard, tap **Network Monitor**. Alternatively, select **menu > Network Monitor**.

3. In the Network Monitor Settings screen turn **Device Network Monitor** ON, and then configure the desired networks.

Configuring a Network

To configure a network, follow these steps:

1. In the Network Monitor menu, tap **Summary** and ensure that **Device Network Monitor** is turned ON.
2. Select a network to be configured.

   NOTE: In this example, Mobile Network is selected.
3. In the Data usage bill date list, tap the date picker to select the billing date.
4. To set data usage limit, select the **Set data usage limit** option.
5. Enter the data limit in the **Alert if data usage reached max limit of** option.
6. Enter the data usage limit in the **Alert if data usage reaches** option to get alerts.

   NOTE: Data usage limit in the Alert if data usage reached max limit option should be equal to or higher than that of in the Alert if data usage reaches option.
7. To stop network once the data usage limit reaches its maximum limit, turn **Stop network usage on max limit reaches** ON.

Chapter 5. Thirtyseven4 Tablet Security Menu

The Thirtyseven4 Tablet Security menu includes all the features of the software. If a feature is not available on Dashboard, it can be found in the menu.

Following features are available under the Thirtyseven4 Tablet Security menu:

General Settings	Helps configure all the features of Thirtyseven4 Tablet Security.
Tools	Helps to view, remove, and restore the Quarantine files, and update the product.
Reports	Helps to view reports of all blocked calls, blocked SMS, Anti-Theft, scans, virus protection, and web security.
Help	Helps to access the Help topics, seek Technical Support, and view the license details of the product.

General Settings

This feature allows configuration of password protection and the settings for notification, Internet, reports, messenger, and web console.

Password Protection

This setting sets the password and password protection to block unauthorized access to the device.

To configure Password Protection, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. Tap menu and then tap **General Settings**.
3. In the General Settings menu, tap **Password Protection**.
4. To enable password protection, turn **Enable Password Protection** ON.
5. Enter password in the **Password** and **Confirm Password** field.
6. To save your settings, tap the **Save** button.

Notification Settings

With Notification Settings, enable alerts for events such as, virus detected, license expiry information, device security status, virus database update, and information about calls or SMSs received from the blocked contact numbers. All these notifications help to take an appropriate action on time.

To configure Notification Settings, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. Tap menu and then tap **General Settings**.
3. In the General Settings menu, tap **Notification Settings**.
4. To enable Notification Settings, turn **Enable Notification** ON.

Internet Settings

With Internet Settings, select and manage any available network on the device.

To configure Internet Settings, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. Tap menu and then tap **General Settings**.
3. In the General Settings menu, tap **Internet Settings**.
4. Select one of the following network; Any available network, Wi-Fi only, or Mobile networks.

Reports Settings

With Reports Settings, configure the reports to be generated on various events of Thirtyseven4 Tablet Security. The reports will be generated automatically depending on the set schedule.

To configure Reports Settings, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. Tap menu and then tap **General Settings**.
3. In the General Settings menu, tap **Reports Settings**.
4. To generate reports, select the number of days from the following options; 7 days, 30 days, and 45 days.

   NOTE: However, 30 days is selected by default.

Virus Statistics Settings

With Virus Statistics Settings, report virus statistics to the Thirtyseven4 server.

To configure Virus Statistic Settings, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. Tap menu and then tap **General Settings**.
3. In the General Settings menu, tap **Virus Statistics Settings**.
4. To report virus statistics to Thirtyseven4 server, turn **Virus Statistics** ON.

Tools

With Tools, update the copy of Thirtyseven4 Tablet Security for the latest virus database.

Update

If the device is connected to the Internet, Thirtyseven4 Tablet Security gets updated automatically for any virus database.

This is helpful if the device was not connected to the Internet or was switched off for few days.

To take the updates, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. Tap menu and then tap **Tools**.
3. In the Tools menu, tap **Update**.
4. In the Update item, tap **Update Now**.

   NOTE: In case there are no latest updates available, the **Up to Date** message is displayed.

Quarantine

Quarantine is a specific folder where Thirtyseven4 Tablet Security places all potentially suspicious, malicious objects. Check the list of quarantined objects to get the details on the object's full name and the date of detection. The quarantined objects can be deleted or restored.

To take action on the quarantined files, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. Tap menu and then tap **Tools**.
3. In the Tools menu, tap **Quarantine**.
4. Do one of the following:
   - **To Remove**: Select the files and tap **Remove** to remove the suspicious files.

     NOTE: Once the files are removed, they cannot be retrieved.
   - **To Restore**: Select the files and then tap **Restore** to restore the files.

Remove personal data

With this option, all the contacts, SMS, calendar, and SD card data can be deleted. This is a secured deletion method where data is deleted permanently.

To remove personal data, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. Tap menu and then tap **Tools**.
3. In the Tools menu, tap **Remove personal data**.
4. Select the data type that is to be removed.
5. Select one of the deletion methods:
   - One Pass – Quick Data Destruction
   - Multi Pass – More Secure Destruction
   - DoD – Standard Data Destruction
6. To remove the selected data, tap **Secure Delete**.

One Pass – Quick Data Destruction	Uses random letters to overwrite the data. This is the best and default file deletion method. Data once deleted cannot be recovered.
Multi Pass – More Secure Destruction	Uses twice the number of random letters to overwrite the data. This method of deletion provides additional layer of security. Data once deleted cannot be recovered by any recovery software.
DoD – Standard Data Destruction	Uses the encryption method of using random letters to overwrite data as per the Department of Defense Memo. Data once deleted cannot be recovered by any recovery software.

Reports

With Reports, view the reports generated on various events as follows:

Blocked SMS	Displays the list of blocked SMSs.
Blocked Calls	Displays the list of blocked calls. For every entry there is a list of last 10 calls, date and time details.
Anti-Theft	Displays Anti-Theft reports such as whether the device was ever blocked on SIM change, device was locked remotely, or data was wiped remotely etc.
Scan	Displays Scan report with information of threat found, location and action taken.
Virus Protection	Displays Virus report with information of threat found, location and action taken.
Update	Displays details of updates taken for Virus Database.
Backup	Displays reports on backup taken or deleted.
Web Security	Displays reports on all activities related to web security such as the blocked sites, malicious sites visited, phishing sites etc.

To view reports, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. Tap menu and then tap **Reports**.

Chapter 6. Technical Support

Thirtyseven4 provides extensive technical support for the registered users in various ways. Access the Help menu to get information about how to use Thirtyseven4 Tablet Security, how to get assistance on any issue from Thirtyseven4 experts, and so on.

Help

The Help menu includes information about the product license, support system, the help topics, and the deactivation option.

To view Help, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. In the menu, tap **Help**.
3. To view the Help topics, tap **Help**.

About

The About screen includes details of the product (Product Name, Version and Virus Database Date) and License details (User Name, License valid till date, etc.) along with the options such as Update Now, Renew Now, Update License, and Update email ID.

Updating License after Buying Renewal Code

To update the product license after buying renewal code, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. In the menu, tap **Help**.
3. Tap **About**.
4. Tap **Update License**.

Technical Support

Thirtyseven4 provides extensive technical support for the registered users of Thirtyseven4 Tablet Security. The Support menu includes the following support systems:

- **Web Support (Visit FAQ)** – Frequently Asked Questions offers answers to the most common queries related to Thirtyseven4 Tablet Security.
- **Email Support (Submit Ticket)** – This is an online Technical Support system that helps to submit the queries and issues.

- **Live Chat Support (Chat Now)** – Chat with our experts online if expert attention is required for the issue.
- **Telephonic Support** –Thirtyseven4, LLC. also provides technical support between 8:00 AM and 5:00 PM EST.

  Thirtyseven4 users can call toll-free +1 877-374-7581.

Email Us: Email your queries and issues to support@thirtyseven4.com.

Logs

Send us the logs for the technical issues to troubleshoot the issue.

To send the logs, follow these steps;

1. Turn the **Enable Logs** option ON.
2. Then tap the **Send Logs** button.

Help

To view the Help topics, follow these steps:

1. Go to **Thirtyseven4 Tablet Security**.
2. In the menu, select **Help** > **Help**.

Deactivation

To remove Thirtyseven4 Tablet Security, first deactivate the product. This will help to re-install and reactivate the product later.

To deactivate Thirtyseven4 Tablet Security, refer Deactivating Thirtyseven4 Tablet Security section.

