

User's Manual





Table of Content

- 1. Key Benefits
- 1. Key Features
- 1. Registration Process
- 1. Scanning of Viruses
- 1. Automatic Online Updating
- 1. Quarantine
- 1. Bluetooth Scanning
- 1. Spyware
- 1. SMS/Email Spam Blocker
- 1. Alerts & Logs

Key Benefits

- ❖ Antivirus, Anti-Spyware and Anti-Spam Protection at one cost.
- ❖ Easy Installation and Activation
- ❖ Automatic scanning and removal of viruses without attending it.
- ❖ Protection for security, archiving, compliance, and Privacy.
- ❖ Protection against the latest threats.

Key Features

- ❖ Provides efficient and complete solution for all types of viruses.
- ❖ Protects smart phones including selected models for Nokia, Panasonic, and other leading manufacturers.
- ❖ Detects and automatically removes viruses, worms, Trojan horses, and evolving malicious code.
- ❖ Built-in firewall monitors all inbound and outbound LAN/WAN communications, blocking suspicious connection attempts.
- ❖ Virus independent – protects against future viruses.

Registration Process

When the user purchases a Mcure Antivirus Application he has to register with the site. First the user has to download the Mcure cab file or exe from the site and install it in his mobile. After successful installation of the application the registration process begins. Now the user has to follow the steps given below at the first launching of the Application in his mobile:

- ❖ A Mcure activation form appears with a request code and will require the user to give the Unlock code.
- ❖ To get the Unlock Code, the user should register the product in the Site.
- ❖ For this he has to give the necessary detail requested for registration and the payment process.
- ❖ Once the payment is successfully made, the site mails the Unlock Code to the user pertinent to the particular request code.
- ❖ Now the user can just enter the Unlock Code and activate the Mcure Application pertaining to his Mobile only.

The product registration is valid for a Single Mobile device only.

Scanning for Viruses

There are different types of scans available to provide additional protection:

On-demand scans:

Using this scanning method, the user can scan a file, folder, drive, or entire directory at any time.

Scheduled scans:

A scheduled scan is an important component of virus protection. At the very least, schedule a scan to run once per week to ensure that your mobile remains virus-free. This virus scan will run unattended at a specified frequency.

Startup scans:

This type of scan will run every time you start your mobile and when windows loads.

Custom scans:

To scan regularly the same set of files or folders, Custom scan can be created and restricted to just those items. At any time, the specified files and folders can be quickly verified for viruses.

Context Scanner:

This feature enables user to scan any file or folder in the mobile using our Mcure. Using the File Explorer the user can explore the content of the mobile and select file or folder to be scanned.

The process to be followed for the Context Scanning are:

- ❖ Open File Explorer
- ❖ Choose any folder by Press and Hold using stylus
- ❖ A context menu appears as popup
- ❖ From the options given in the Context Menu, select “Scan with Mcure”
- ❖ On selection the Application will start to scan the particular Folder or File
- ❖ At the end of the Scan, result is displayed with an option to delete or quarantine the viruses, if any.

Automatic Online Updating

The mobile applications will be intimated about the new updates available in the server. The user can manually download the updates or setup a scheduled updates download.

The application will interact with the server frequently to check whether the setup running in the client device is up to date. If not, the updates will be downloaded and added to the virus definitions. The automatic update process will update its industry-leading definitions database to keep you protected against these threats.

Quarantine

The virus infected files will be automatically quarantined /segregated to a separate folder or manually intimating the mobile user about the whereabouts of virus infected file.

After quarantining, virus definitions need to be updated, so as to treat the infected file. To avoid data loss during cleaning process, a backup of the infected file will be kept separately. After successful cleaning of the infected file, the corresponding backup file will be deleted.

The clean files will be moved to their former folder locations. If the folder locations are not present, it will be placed in the “Repaired items” folder.

Sometimes, a new virus would have infected the user’s mobile. In such cases, intimation will be sent automatically to the development center to analyze it to make sure the type of virus that infected the file. The development team would find a solution to eradicate the latest virus from the user’s mobile.

Bluetooth Scanning

Certain viruses will distribute through Bluetooth connections, attacks operating system of mobiles. This virus will scan for phones that are using the Bluetooth technology to get spread.

The event listener is a feature which monitors all the data transfers, file execution & manipulation. This keeps track of all the data transactions occurring to and fro. If there is any virus infected data, it will alert the user.

After user approval, the virus infected file(s) will be quarantined to a separate location in the mobile memory. The virus cleaner will take necessary actions there on.

Spyware

Spyware is a software that covertly gathers user information through the user's Internet connection without his or her knowledge.

Anti-Spyware programs will combat Spyware in two ways:

1. Real-time protection which prevents the installation of Spyware.
2. Detection and removal, which removes Spyware from an infected mobile.

SMS / E-mail Spam Blocker

Spam Blocker is a feature that enables the device to ward off Spam E-mails and Messages from entering the Mobile.

SMS Spam Blocker

The SMS spam blocker features enables the device to block all the SMS's that are classified as "Spam" by the user. The messages can be blocked using 2 criteria's namely Sender Name & Address and Body Content.

Enabling the SMS Spam Blocker

There are two methods by which the Spam settings for SMS can be enabled. Firstly, the user can open the Mcure application and move to spam settings. Here he can select the Sender option and enter the Name & Address of a contact and enable as Spam. The other option is to Press and Hold the Messages or SMS in Inbox, on which a Context Menu appears with an option "This is Spam". If the user selects this option then the Application automatically makes note of the Sender Number and in case of future SMS transfer from the Particular Sender our application moves the SMS to Spam Folder.

Incase of Body Content, the user will navigate to the Language in SMS Spam Settings and give Words or Phrases, which are to be considered as Spam. Once he makes such settings the Spam blocker automatically blocks all the messages with such "Words or Phrases".

E-mail Spam Blocker

The Email spam blocker is a feature enables the device to block all the Email's that are classified as "Spam" by the user. The messages can be blocked using 3 criteria's namely Sender Name & address, body Content and Domain.

Enabling the Email Spam Blocker

Firstly the user can open the Mcure application and move to Email spam settings. Here he can give Email Address, mails from a Particular Domain and Body Content.

The other option is to Press and Hold the Emails in Inbox, on which a Context Menu appears with an option "This is Spam". If the user selects this option then the Application automatically makes note of the Sender Email ID and in case of future Email transfer from the Particular Sender, our application automatically moves the Email to Spam Folder.

In case of Body Content, the user will navigate to the Language in Email Spam Settings and give Words or Phrases, which are to be considered as Spam. Once he makes such settings the Spam blocker automatically blocks all the Emails with such "Words or Phrases".

Alerts & Logs

When a new virus is blocked by the user's anti-virus application, it will automatically send a notification message to the server. Thus, by intimating, it helps the development team to react fast on the new threat and to find out a solution for it. This notification can be de-activated or made manually notified.

Log will be maintained for each and every scanning operation done in the mobile phone. These log files will help in getting a statistical report of the virus attack during a particular period and also to be noted about the new threats to the mobile.