Max Secure provides a New World of Proactive Protection for Your Computer and Mobile
User Guide

Thank you for choosing Max Total Security to keep your Windows PC safe and protected from all types of virus and Malware. This document will be revised as and when required due to product modifications. This document will help you understand how to use this product quite thoroughly.

This document is the property of Max Secure Software India Pvt. Ltd all rights to this document are reserved by the copyright laws of the Indian Federation and by international treaties. Illegal reproduction and distribution of this document or administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Max Secure Software India Pvt. Ltd.

Max Secure Software Pvt. Ltd. reserves the right to amend this document without additional notification. This document, and graphic images related to it, may only be used for informational, non-commercial, and personal purposes only.

Max Secure Software Pvt. Ltd. assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document to which rights are held by third parties, or for any potential damages associated with the use of such documents.

This guide will help you install, activate, uninstall and use Max Total Security.

Document revision date: 27 August 27, 2015

Max Secure Software India Pvt. Ltd. All Rights Reserved.
http://maxsecureantivirus.com
Table of contents

1. How to get Max Total Security ........................................................................... 6
   a. System Requirements ............................................................................... 6

2. How to Install ..................................................................................................... 7
   a. Install from CD ...................................................................................... 7
   b. Install from Internet ............................................................................... 7
   c. Install using command line (CMD) ....................................................... 7
   d. Installation Procedure ........................................................................... 8
   e. Un-installation Procedure .................................................................... 9

3. How to Activate Product .................................................................................... 10
   a. How to Register .................................................................................... 11
   b. Internet Registration ........................................................................... 12
   c. Off-Line Registration ......................................................................... 13
   d. SMS Activation .................................................................................... 14
   e. Phone Activation .................................................................................. 15
   f. Chat Activation ..................................................................................... 15
   g. Email Activation .................................................................................... 15
   h. Remote Support Activation .................................................................. 17
   i. Renewal Registration ........................................................................... 17
   j. Activating from command Prompt ....................................................... 18

4. How to Update .................................................................................................... 19

5. Scanning Computer .......................................................................................... 21
   a. How to Scan .......................................................................................... 22
   b. Quick Scan ............................................................................................ 23
   c. Custom Scan .......................................................................................... 23
   d. USB Scan ............................................................................................... 23
   e. Full Scan ................................................................................................ 24
   f. Deep Scan ............................................................................................... 25
### 6. Protection Center
- **Network Filter**: 37
- **Application Rules**: 38
- **Internet Filter**: 39
- **Email Scan**: 40
- **Network Monitor**: 43
- **Parental control**: 44

### 7. Live Update
- **Update using Internet**: 48
- **Update using Local Network (Intranet)**: 49
- **Off-line Update**: 49

### 8. Support
- **LapTop Tracker**: 51
- **Tell a Friend about this Software**: 52
- **Renewal process**: 52
- **Live Chat**: 52
- **Remote support**: 53
- **Export Log**: 53

### 9. Max Shield
- **IE Home Page Protection**: 55
- **Tracking Cookie protection**: 56
- **Active Monitor protection**: 56
- **System File protection**: 56
- **File Association Monitor**: 57
- **Windows restrictions protection**: 57
- **Enable/Disable Active protection**: 58
- **IE restrictions protection**: 58
10. Settings........................................................................................................................................ 60
    a. Custom Settings.................................................................................................................. 60
    b. Advance Settings ............................................................................................................. 61
    c. Proxy Settings .................................................................................................................. 63
    d. Scan by Name ................................................................................................................... 64
    e. Product Info ...................................................................................................................... 66

11. Options....................................................................................................................................... 67
    a. Exclude-Recover Options .................................................................................................. 67
    b. Exclude Options ................................................................................................................ 67
    c. Cookie / BHO Options ...................................................................................................... 68
    d. Recover Options ................................................................................................................ 70
    e. Registry / Hosts File Options ............................................................................................ 72
    f. Net Fix Options ................................................................................................................ 74
    g. Process Entry Options ...................................................................................................... 75
    h. Startup Entry Options ...................................................................................................... 77

12. Tools.......................................................................................................................................... 79
    a. USB Manager Tools.......................................................................................................... 79
    b. Browser Fix Tools ............................................................................................................ 81
    c. Max LiveUpdate Fix .......................................................................................................... 82
    d. IE Explore Fix Tools ......................................................................................................... 83
    e. Registry Backup Tools ...................................................................................................... 84
    f. Registry Fix Tools ............................................................................................................. 85
    g. Services Tools ................................................................................................................... 85
    h. System Volume Information Cleaner .............................................................................. 86
    i. Security Vulnerability Scanner ......................................................................................... 88
    j. Rootkit Scanner ................................................................................................................ 89
    k. Restore Point Creation ..................................................................................................... 90
    l. Unhide Folder Tool ........................................................................................................... 91
    m. PC Tuner .......................................................................................................................... 92
    n. Safe Browser ................................................................................................................... 93
    o. Virtual Keyboard ............................................................................................................. 94
    p. Data Backup utility .......................................................................................................... 95
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td><strong>PC Tuner</strong></td>
<td></td>
<td>92</td>
</tr>
<tr>
<td>14.</td>
<td><strong>Safe Browser</strong></td>
<td></td>
<td>93</td>
</tr>
<tr>
<td>15.</td>
<td><strong>Virtual Keyboard</strong></td>
<td></td>
<td>94</td>
</tr>
<tr>
<td>16.</td>
<td><strong>Data Backup Utility</strong></td>
<td></td>
<td>95</td>
</tr>
<tr>
<td>17.</td>
<td><strong>Short-cut Keys</strong></td>
<td></td>
<td>99</td>
</tr>
<tr>
<td>18.</td>
<td><strong>Discussing on forum</strong></td>
<td></td>
<td>99</td>
</tr>
<tr>
<td>19.</td>
<td><strong>Security Blog</strong></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>20.</td>
<td><strong>Feedback</strong></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>21.</td>
<td><strong>Useful Links</strong></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>
HOW TO GET MAX TOTAL SECURITY

You can buy this software in the following ways:

- Buy CD in a Box along with the registration key from any computer Dealer
- Online from our website http://maxsecureantivirus.com/mts/index.htm

ABOUT MAX TOTAL SECURITY

Max Total Security provides complete protection against all types of Malware, Network attacks, phishing and Spam. It includes following features:

- Anti-Virus and Anti-Spyware Scanner
- Active Protection
- Firewall
- Parental control
- PC Tuner
- Data Backup

WHAT DO YOU GET

- Daily threat definition updates
- Free product upgrades
- 24x7 technical Support help, Telephonic, Live chat and Remote Desk top support

HARDWARE AND SOFTWARE REQUIREMENTS

- 1 GB Hard disk space, 512 MB RAM
- CD/DVD-ROM FOR installing software
- Internet access for updates and online activation
- Internet explorer 6.0 , should be online mode
- Windows 10, 8.1, 8.0, 7, XP, Server 2008 R2, Server 2012 Server 2003 ; 32 and 64 bit versions
INSTALLING AND REMOVING THE APPLICATION

This section contains instructions for application installation and removal. Set up files can come from CD or Internet download.

INSTALLATION PROCEDURE

Installation can be done from CD or files downloaded from Internet file. Installation can also be started by command prompt in silent or visible mode.

INSTALLING FROM CD

As soon as CD is inserted in CD ROM, set up launches and starts installation. First step is to choose the localization language. During this step the Setup Wizard prompts you to view the License Agreement concluded between you and Max Secure Software, you need to click on Yes to continue. Read the License Agreement thoroughly and, if you agree with all of its terms, click the I Accept the Agreement. Next step will ask you whether you want to participate in Max Secure Threat Research Community. Checking this option Yes, allows us to scan your PC for new threats existing on your PC and not yet detected. This helps us detect newer virus samples and achieve zero day threat detection goal. As soon as we get these samples, we process them and release virus definition updates for all the other users.

If the terms of the License Agreement are not accepted, the application will not get installed.

INSTALLING FROM INTERNET

If you have downloaded set up from internet using download manager from the website http://maxsecureantivirus.com/ then that downloads files and starts installation. Rest of the steps are the same as above, wizard continues and asks you to accept the agreement and installs very quickly in about 3-4 minutes.

INSTALLING USING COMMAND LINE

Installation can be done from command line once you have downloaded set up file or have setup on cd in your PC.

You need to start cmd prompt from Start>Run>cmd and give the file name along with the path and add /verysilent if you want to install in silent mode. Command prompt will look like C:\users\admin\MaxTSx64.exe, see illustration below:
INSTALLATION PROCEDURE

You start installation by any of the above means, first installer checks for the presence of any other anti-virus products on the computer. It is called compatibility check. If any other anti-virus applications are detected, you can choose to remove them. Removal of other Anti-Virus products is done automatically by the installer if you select yes.

It is advised to keep only one anti-virus product on your PC as many anti-virus on one PC can significantly slow down and hang your PC.

When removing incompatible applications, you will need to restart your PC, after which installation of Max Secure Total Security continues automatically. You need not launch the installer.

As soon as installation starts, installer launches a Memory scanner to check for the presence of any malware in running process to make sure that installation process goes through successfully 100%, without any chance of infections. You may choose to cancel this scan and continue with the installation if you are sure that there are no malware present on your PC.
UNINSTALLATION / REMOVAL PROCEDURE

Please note that after removing Max Secure Total Security, your computer will not be protected from malware.

Uninstalling product is very easy. You can uninstall from Control Panel>Max Total Security>uninstall. You will be asked if you want to keep the quarantined files, in case you wish to recover the malware files later. You can say Yes or go for No for the complete removal of quarantined files.

On Windows 8.1, go to Start menu, on the Apps screen, right click Max Total Security >Uninstall. If you have added any password to Parental Control or Firewall then you will be required to enter it before you can uninstall. Reboot will be required for the full removal of all the files.

PRODUCT ACTIVATION

Activation process lets you use all the features of the product and make it fully functional for the time period that it is activated.

If you have purchased a license for Max Secure Total Security Online then registration key is immediately sent to you by email. You need to register the product using this registration key.

If you bought the product box from a store then registration is included inside the box along with the CD.

There are several options for activating the product:

- **Register Now.** Select this button and enter Registration No. if you have a Registration key for the product On-line or Off-line.

- **Activate trial version of the application.** Select this activation option if you want to install the trial version of the application before making a decision on whether to purchase a license.

  You will be able to use the application and all of its features during a short evaluation period of 30 days. When the trial license expires, the trial version of the application cannot be activated for a second time on the same PC. You need to have valid Registration key to activate it once Trial period is over.

**Note:** 1. An Internet connection is required for activation of the application.
HOW TO REGISTER

Launch product from the system tray or short-cut on the desktop

While you are registering the product, please check that you are connected to the Internet. Product needs to connect to Registration server to activate your copy of the product.
INTERNET (Online) REGISTRATION

Click on the **Register Now** button, this will open the Registration window:

- Enter your details - First Name, Last Name, Address, Phone No, Date of Birth, E-Mail Address.

Click on Next Button to go step 2 and fill Registration No. here:
• In the text box "Registration No" enter the Registration Number. Please Note:
  
a) Copy and paste the Registration Number to ensure exact data entry, do not type it in.
  b) Please make sure that all information is entered to the far left of the textbox fields and that there are no blank spaces to the left.

• Renewal No.: 
  Registration number has a time validity and once that period is over then 15 days prior to expiration a message is displayed to renew the subscription. Hence a renew key is required to renew subscription for already existing registered user. After obtaining renew key, copy the key and paste it in renew key box. Then click on Activate Now button.

  Online user can purchase renew key by clicking renew now button shown in product. For offline users, renew key can be obtained by buying a new product box from many dealer.

• Dealer Code: Every authorized dealer is assigned a code or id which should be filled here for easy tracking of dealer’s customers, their renewal and tracking.

OFFLINE REGISTRATION METHODS

There are many ways in which a user can activate product even if he does not have internet. Clicking on offline registration opens this page:
SMS ACTIVATION

On your mobile, type max 9QDF-XZ1C-N129-A605-EAF9 123QWERT5663, (see below, this code will be different on your PC)

- **Installation Code**: This contains PC hardware information, which is unique for every computer. This is used for off-line registration for customers who do not have internet available.

- **Activation Code**: Activation code provides information to activate the product. Mostly used by off-line registration.
PHONE ACTIVATION

Register by calling our technical support, click on Phone button and provide them this information and they will give you activation code, fill that here and click Activate now. Product will get registered.

CHAT ACTIVATION

Click on Chat Button, it will open Max Secure chat window. By filling your name and email id, you can get on live chat with our technical team person. He will ask you to give him information required to register product.

EMAIL ACTIVATION

If you are having difficulties with the product activation, then click on E-mail Button, it will open window like this. Clicking on Send Email button will send us mail.
If you click on **Offline** Button, it will open window like this:
REMOTE SUPPORT:

You can remotely connect to Max Secure support and have them access your desktop to fix issues by clicking on the Remote Support button 24x7.

![Remote Support](image)

RENEWAL

10 days before your subscription expires or if your subscription has already expired, a Buy now button will be displayed.

We value our existing customers and want them to stay protected against latest threats so we remind them by a system tray notification, once a day to renew the subscription. If you do not Renew after product activation expires, you will no longer be protected. You will not lose any subscription days even if you activate many days before product expires. Remaining days will be added to the new subscription.

Clicking on Buy Now will take you to a purchase page. If you have already purchased a license then click on Renew Now to activate product using any of the activation methods described above.
BENEFITS OF REGISTRATION

Registered users can get free Technical Support help for any issues on their PC related to our products or malware infections, manage activation codes, and receive the latest information about new updates, newsletters and special offers from Max Secure Software.

ACTIVATING FROM THE COMMAND PROMPT

You can register Max Total Security from the main interface Register Now button or from command prompt.

Command prompt syntax:

1. Enter the First Name
2. Enter the Second Name
3. Enter Email Address
4. Enter Registration No

All above information is mandatory.
Result of Registration will be displayed. See the example below:

![Registration Result]

---

**COMPLETING ACTIVATION**

Once activated by any of the methods above, the Wizard informs you that Max Secure Total Security has been successfully activated. In addition, information about the current license is provided in the Support window accessible from main user interface.

**UPDATING PREVIOUS VERSION APPLICATION**

When you buy a CD it may not be as updated as online version. It is recommended that after installation you update the program to reflect the latest definitions. There are two ways for updating this program:

1. Right click on system tray icon and click on live update option after clicking on live update option live update GUI is opened, then Click on Update Now button. After completion of live update, message will be displayed with “Live Update Successfully”.
2. At the top right corner of screen there is Max Total Security program gadget for easy access to most commonly used features. Choose the center option, download Updates. After choosing live update option, live update user interface (UI) will open. Click on Update Now button. After completion of live update the pop up message display with “Live Update Successfully”. 
SCANNING THE COMPUTER

This section provides information about how to scan your computer for viruses and other threats. **Max Secure Total Security** scans your system and looks for traces of virus and spyware components. Its threat definition database is updated several times a day on an incremental basis with details of newly found, most prevalent threats reported in our encyclopedia on this website [http://thespywaredetector.com/spywarealpha.aspx](http://thespywaredetector.com/spywarealpha.aspx).

Max Secure Total Security also deploys various other techniques using an updated database and heuristic approach.

In addition to Active monitoring which is always ON, Max Secure Total Security scans for the threat entries in the following locations:

- Registry
- Cookies
- Files
- Folders
- Processes
- Hidden Entries
- Memory

Some threats modules/components load themselves in the memory with other processes such as explorer.exe or winlogon.exe etc. Such infected files are shown in the Max Secure Total Security user interface along with the processes they load themselves. Max Secure Total Security identifies and cleans such threat processes. These findings are written in the Max Secure Total Security log as well. It will be notified in the user interface of Max Secure Total Security as Threat Type: Memory.
HOW TO SCAN YOUR COMPUTER

Launch Max Secure Total Security by clicking on the Start>Programs > Max Secure Total Security. Alternatively, you may wish to start Max Secure Total Security by double-clicking on a shortcut icon on your Windows Desktop. On windows 8.1 you can also launch Max Secure Total Security from the app menu screen. After launch, first, the Tips window opens with a "Tip of the Day".

- You can choose to read more than one tip by clicking on the "Next tip" button or “Close” and open the main interface immediately.

- If you do not wish to view the Tips window each time you start Max Secure Total Security, simply uncheck the checkbox before the "Show tips at startup" text or go to Settings> Custom Settings> uncheck "Show tips at startup" option. You can turn this feature ON or OFF at any time by selecting this checkbox again.

- The main window of Max Secure Total Security will open along with the Scan Options Window on top of it. There are three scan related buttons on the Scan Window: Quick Scan, Full Scan, Custom Scan and Mobile Scan. Click on the scan option you want to perform and scanning will start.
• **Shutdown computer after scan is completed**

If you select this option then, Max Secure Total Security will automatically shut down your computer after scan is completed. Not available in Quick Scan because that scan finishes in about 2-3 minutes so not required.

• **Quick Scan**: will scan critical locations and memory of the current operating system drive only (i.e. Only C drive).

• **Custom Scan**: will scan only the file/folder locations selected by the user.

• **USB Scan**: will scan as soon as any Pendrive is connected to your PC in the USB port. You have an option to turn off automatic scan from Tools> USB Manager.
Full Scan: will scan your complete PC including the operating system, program files as well as your files and documents. If your PC has more than one hard drive on it, you can select which hard drive you would like to scan in the Full Scan option. This is done by checking the appropriate checkbox before the hard drive letter (e.g. C:) in the Full Scan window.

On Full Scan window, you would see Deep and Critical scan selection check boxes
DEEP SCAN: Deep Scan option does thorough scanning throughout the drive so that Max Secure Total Security catches more special threat entries. It takes more time in first scan but subsequent scan will take less time to scan special threat on the drive.

CRITICAL SCAN: Select this option only when your pc is heavily infected. Critical scan suspends all the processes using heavy cpu resources and makes scanning faster so that you can find threats as soon as possible.

- While Max Secure Total Security scan is running, if you want to pause scanning for some time then you can do it by clicking on the Pause button. When you wish to resume scan then click on the Resume button. You can stop the scanning by clicking on the Stop button.

- If you have an unregistered copy of Max Secure Total Security, then the following window will open after the scan is completed. You will be need to Register to delete the infected threat entries found on your PC. Click on Fix Issues Now button to register the Max Secure Total Security.

You will be presented with the options to register
• Clicking on the Register Now button opens Registration window, where you can fill your first name, last name, email address and the product registration number mailed to you or registration number from the product box when you purchased Max Secure Total Security.

• If you do not have the registration key, click Order now to buy new subscription. You will receive a product registration number by email after the purchase.

• You can also choose to go for Free 30 day trial.

• You can click Skip to do none of this and open the main interface.

• Main window also allows you to Buy, Register or Renew your copy of Max Secure Total Security.
• After you register your copy of Max Secure Total Security, you can start Scan, do Live Update, go to Protection center and turn on Firewall or contact support by using different options on Support window. All these options are easily accessible from the main interface. You can also see few more buttons on the bottom of the screen like Max Shield, Settings, Options and Tools which provide many features.

• You can contact our Technical Support team on 24x7 Live Chat service by clicking on Live Chat button.

• Clicking on Help button (? On the top bar) will open Max Secure Total Security's Help file.

SCHEDULER:

• This option lets you schedule scans of your PC. Max Secure Total Security will run the scan at the time set by you. You can also specify what action Max Secure Total Security needs to take when it detects any threats during such scans.

• This option is useful when you would like your PC to be scanned at regular intervals - daily or weekly for instance. You can prefer to set the scan to occur when you are not using your PC.
Scheduler keeps you protected every day without you having to even open the application. You can also cancel a previously set schedule by clicking the Cancel Schedule button.

The Scheduler window has the four action item fields as given below, select the options you want and click on the OK button to schedule the scan.

**Action Items**

- **Scan Options**
- **Scan Time**
- **On Detection**
- **After scan is complete**

**Scan Options:**

Following options are available:

- **Quick Scan:** Scans the hard drive where the operating system is installed.
- **Full Scan:** Scans all the selected hard drives present on the computer. You can also select the Individual drive or all the drives for scanning.
- **Deep Scan:** Deep Scan is thorough scan to detect most hidden malware.
Scan Time:

Select Daily, Weekly, Hourly or Minutes schedule to scan your PC.

On Detection: This section has two options,

i. Log Only: If you select this option then, Max Secure Total Security will scan your PC for the threat and only show you the log of the detected threat at that time.

ii. Clean: If you select this option then, Max Secure Total Security will scan your PC for the threat and directly clean the threats detected on your PC.

After scan is complete:

i. Shut down the computer: If you select this option then, Max Secure Total Security will automatically shut down your computer after scheduled scan has completed.

ii. Log off from the computer: If you select this option then, Max Secure Total Security will automatically log off your computer after scheduled scan has completed.

NOTE: If your PC is off at the scheduled time, Max Secure Total Security will start scanning whenever your PC is started next.

REPORTS

This option contains the list of threats that are found during the current scan. If Auto Clean is OFF from (Settings>Enable Auto Clean) then you can clean detected threats manually by clicking Clean button here.

SCAN STATISTICS

Max Secure Total Security shows Scan Statistics to summarize total count of different types of threats found since the installation of Max Secure Total Security.

By Clicking on View Scan Statistics link, you will be able to view threats severity detected on your PC so far.
The detected threat entries are flagged under four threat levels which are defined below.

- **Critical**: May open up communication ports; use polymorphic tactics, stealth installations, Rootkit and/or anti-spy counter measures. May contain a security flaw. Requires Special means to remove it. Virus, Spyware and Fake Anti Spyware may fall under this category.

- **High**: Hard to remove, downloads and installs other applications, has the ability to phone home information. Logs keyboard activity, takes system snapshots. Logs activities and removal is difficult. Dialers and Keyloggers may fall under this category.

- **Medium**: May profile users or broadcast data back to a server with ("opt-out") permission. Removal is hard. May show pop-ups which may be contextual or random. May be bundled with other legitimate software. Usually download with p2p and free shareware application. Usually Adware, Backdoor, Trojans, Browser Helper Objects, Toolbars, and Worms may fall under this category.

- **Low**: No immediate threat, may profile users, but has specific privacy policies in place. Not so dangerous, fairly easy to remove, using standard "Add/Remove Programs" function. May make use of "drive-by installation". Removal is possible by end
user. Usually cookie, Droppers, Flooder, hacker tool, hijacker and Downloader fall under this category.

By Clicking on Last Scan History button present on main UI, you will be able to view Scanned threats history in a List.
MOBILE SCAN

Scans mobile phones for malicious threats if they can connect to your PC.

Scanning from Command Line

Max Secure Total Security offers users the ability to run a scan from the command line.

Why command line scanner

Run in Standalone mode. If your PC is highly infected and not able to open user interface then you can execute command line scan. If you still cannot run Max Secure Total Security then we would suggest you to do scan in the Safe mode with command line scanner.

Do multiple time scanning automatically by using batch file.

Usable on multiple OS. No dependency on UI.

Max Secure Total Security Command line scanner also works in Safe mode with command prompt.
The following parameters are available for the command line scanner with the syntax:

User can set the following arguments.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/D</td>
<td>Start DataBase Scan</td>
</tr>
<tr>
<td>/S</td>
<td>Start Signature Scan</td>
</tr>
<tr>
<td>/V</td>
<td>Start Virus Scan</td>
</tr>
<tr>
<td>/K</td>
<td>Start Keylogger Scan</td>
</tr>
<tr>
<td>/X</td>
<td>Recover Threat</td>
</tr>
<tr>
<td>/V /C</td>
<td>Start Custom Scan</td>
</tr>
<tr>
<td>/P</td>
<td>Prompt to user for Clean the entries &amp;To Recover entries</td>
</tr>
<tr>
<td>/A</td>
<td>Start Auto Clean</td>
</tr>
<tr>
<td>/DRIVES:</td>
<td>Select Drives e.g. /DRIVES: C:</td>
</tr>
</tbody>
</table>

If parameters are not set then it displays the usage of Command line Scanner.

Here are some parameter examples you can use right away:
### Command Line Scanner

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Quick Scan</td>
<td>/D /P /DRIVES:C:</td>
</tr>
<tr>
<td>For Full Scan</td>
<td>/S /V /D /K /P /DRIVES:C:</td>
</tr>
<tr>
<td>For Custom Scan</td>
<td>/V /C /DRIVES:&quot;D:\Folder Name&quot;</td>
</tr>
<tr>
<td>To Recover</td>
<td>/X /P</td>
</tr>
</tbody>
</table>

**Quick Scan**: MaxCMDScanner.exe /D /DRIVES: C:

**Full Scan**: MaxCMDScanner.exe /S /D /K /DRIVES: C:

**Custom Scan**: MaxCMDScanner.exe /V /C /DRIVES:"D:\Folder Name"

**Recover Threat**: MaxCMDScanner.exe /X; to Recover all Entries

**How to use Command Line Scanner scan:**

1. Access the Windows Command Prompt. Go to **All Programs>Accessories>Command Prompt**
2. Navigate to the Max Secure Total Security program folder, type MaxCMDScanner.exe
3. To run a parameter, type MaxCMDScanner.exe [parameter].

   For example, if you want to do Quick Scan then type “MaxCMDScanner.exe” /D /DRIVES:C:

**Warning**: Once you start a scan, do NOT manually attempt to terminate it. The scan MUST be allowed to complete to avoid errors. Once the scan completes you will get the message of completion.

**If you want to stop the scan please press ESC (escape) button.**
**CONTEXT MENU SCAN**

Any folder or file can now be scanned at any given instance with the help of Max Secure Total Security Explorer Plug-In. Right click on the folder/file and select **Scan with Max Total Security** to scan that folder/file. With this type of scan, only the selected folder or file will be scanned.

**PROTECTION CENTER**

**What is Firewall?**

A firewall is a piece of software or hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. If you are a home user or a business user, using a firewall is the most effective and important first step you can take to help protect your computer.

The Internet, like any other society, is plagued with the kind of jerks who enjoy the electronic equivalent of writing on other people’s walls with spray paint, tearing their mailboxes off, or just sitting in the street blowing their car horns. Some people try to get real work done over the Internet, and others have sensitive or proprietary data they must protect. Usually, a firewall’s purpose is to keep the jerks out of your network while still letting you get your job done.

Max Secure Firewall provides a robust way to effectively filter Network Traffic, Monitor network activity and take action such as close connection to that network ip, Block applications you do not want to run, Anti-Banner, Anti-Phishing, Block websites you do not want to be browsed, Email Protection, prevent malicious behavior over various protocols, protect running processes, filter web content and Parental control. It provides filtering of I/O requests at the kernel and user levels. Max Secure Firewall is one of the best defenses against malicious software attacks on your system.

**Steps to Enable Protection Center**

Click on Protection Center button present on Main interface. You will see a message window like this:
• Click on Yes, starts configuring Protection center.

• Please wait until you get the following message box.
Note: Please restart your PC once to enable firewall settings

**NETWORK FILTER**

- The firewall keeps track of all communications that have originated from your computer, and it prevents unsolicited traffic from reaching your computer. The two-way firewall monitors your computer’s inbound and outbound connections and prevents local and remote unauthorized network access using many different protocols. You can configure if you wish to block communication from a range of network addresses or protocols.

- A set of rules are provided for specific well-known protocols. This is provided for convenience so that user doesn’t have to have deep protocol knowledge to configure them.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Action</th>
<th>Owner</th>
<th>IP From</th>
<th>To</th>
<th>Port Fd</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP</td>
<td>Allow</td>
<td>System</td>
<td>6.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ping</td>
<td>Allow</td>
<td>System</td>
<td>6.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>OPerating</td>
<td>Allow</td>
<td>System</td>
<td>6.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DHCP</td>
<td>Allow</td>
<td>System</td>
<td>6.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DNS</td>
<td>Allow</td>
<td>System</td>
<td>6.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VPDN</td>
<td>Allow</td>
<td>System</td>
<td>6.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BCAST</td>
<td>Allow</td>
<td>System</td>
<td>6.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LDAP</td>
<td>Allow</td>
<td>System</td>
<td>6.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Allow</td>
<td>System</td>
<td>6.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NETBIOS</td>
<td>Allow</td>
<td>System</td>
<td>6.0.0.0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Following ports are essential for basic features of Windows os, so make sure that you do not block these ports:

1. port = 10001
2. port = 10002
3. port0 = 10003
4. port1 = 10004
5. port0 = 10006
6. port1 = 10007
APPLICATION RULES

- This is a set of rules that manage how certain applications will access the network. These rules are based only on the application path; they don’t configure any port/protocol. They can allow all communications coming to/going from the application. You can add any network application by clicking on Add button and specify rule such as allow or block. Blocked application will not be allowed connect to Internet or Intranet on this PC.

- A firewall will help protect a computer on a wireless network, but will not restrict access to the network itself. You security on wireless network, you should configure your wireless network to use a network key using either Wi-Fi Protected Access (WPA) or wired equivalent privacy (WEP).

There are 4 options when you click Application Rules>Add

Allow:

This option will let you add applications which you want to allow in the Firewall

Block:

This option will let you add applications which you want to block in the Firewall by giving full application path and name of the application.

Ask:

This option will let applications ask you when you try to launch them, if you want to allow or block

Permanent Block Feature: If you want to block any application rule for any application where you are not sure about the application exact path, as expected in the above 3 options, then you can add that rule in this format. You should add “*\” before the name of the rule that you want to block permanently. For an example, by adding “*\iexplorer.exe” you can permanently block internet explorer. Wherever the file is present in your computer will be blocked permanently.

Note: This feature blocks only applications which use network communication such as browsers, chat programs, online games etc.
For Windows 2000 Server, Windows 2000 Advanced Server and Windows 2000 Professional the following Microsoft updates are required:

1. File Name: Windows2000-KB891861-v2-x86-ENU
   Minimum Operating Systems required: Windows 2000 Service Pack 4
2. File Name: Windows2000-KB824151-x86-ENU
   Minimum Operating Systems required: Windows 2000 Service Pack 4

**INTERNET FILTER**

Protects from incoming web traffic, dangerous scripts and malicious URL’s.

Anti Phishing, Anti Banner and Bad Website blocking: This feature protects the incoming web traffic and prevents dangerous scripts and urls from being browsed on your PC added by our malware research team. You can also add your list of urls by domain name or any sub-string if you want.

**Anti Banner:**

Blocks advertising information located on web banners on web pages mostly in browsers. Not only are banner ads devoid of useful information but they also distract you from your work and increase the amount of traffic on your computer.

**Anti-Phishing:**

Protects you from phishing. Phishing generally consists of e-mails from fake financial institutions that contain links to their websites which look alike some genuine bank or financial institution.

The message text convinces the reader to click the link and enter confidential information in the window that follows, for example, a credit card number or a login and password or an Internet banking site where financial operations can be carried out.

**Block Website:**

The module is designed to provide safe Internet surfing by restricting access to unsecure web resources, websites which have been considered as suspicious or phishing.
EMAIL SCAN

Email Scanner is an email security and anti-spam program for all Outlook version before Office 2013.

Malwares spread infection while user opens them considering them to be a legitimate file. If Email Scan protection is ON, it prevents malware infected emails and attachments.

- **Email Protection**
  a. Scans all incoming and outgoing messages and their attachments. POP3, SMTP, IMAP, MAPI and NNTP protocols are supported.
  b. It can block all email attachments if user selects that.
  c. User can check **Block attachment** then click on Settings to add, edit and delete and choose which extensions to block.
- **Anti-Spam** function marks all the emails found as SPAM with the default tag !SPAM but user can change this tag and type here in the text box. Mails contain phishing elements or URL of bad websites or blocked phrases are considered as Spam.

- The incoming mail will also be considered as spam if it comes from the blocked sender or if it is not addressed to the particular user. This feature is highly configurable. Here user can create rules by simply checking options/rule based on if the incoming mails is Spam or not. For example if it comes from allowed sender or it contains allowed phrases or not addressed to me or contains phishing elements etc.

Note: You can turn Email protection ON/OFF from system tray.
• User can also change the label in the body of every mail scanned default setting is “This email was scanned by Max Secure Total Security”. Every email good or spam is marked with this tag.

• For Microsoft Outlook users **Outlook plugin** is added, checking this ON, will move unwanted and SPAM mails to junk folder. If the incoming is a Spam mail then it moves to the Junk E-mail folder instead of the inbox. User can change this folder.
Recover Email:

You can recover suspicious and malicious deleted attachments. Recovered email content will be saved on desktop.

NETWORK MONITOR

- This functionality helps you monitor the entire network (when your PC is connected in workgroup) when you want to block particular PCs due to some security or personal reason.

- To get the benefit of this functionality first you should click on the **Network Monitor** in Protection Center option.

- After clicking on the Network Monitor tab following window will be opened.
PARENTAL CONTROL

Parental Control allows parents to control for how much time children get access to their Computer or Internet and what they do on Internet.
Parental Control Password

- Click on Enter password text box to create your Password.
- Re-enter the password.
- Click on OK button.

Configuring Settings

- Click on Parental Control button present in Protection Center on main interface.
- You can enable Parental Control for all users or for an individual account.
- Click on an individual account, click to turn the switch ON
- Click on Tools image, configure Parental Control settings.
  a. You can turn Firewall ON/OFF from system tray.
Categories:

You can restrict websites as per category. By clicking on a particular category, user can block most popular websites under that category. Check box “Block Websites …”.

Blocked Websites

Click on Blocked sites button, click Add>type specific websites address you wish to block>click Save.

By adding substring you can block websites containing those stings in the domain name.
Internet Usage

If you want to limit the time frame in which user has Internet access or limit the overall time spent on the Internet (for example, 4 hours) or specify the required overall time on the Internet for every weekday (for example, from 5pm to 9pm Mondays – Fridays and From 6pm to 11pm Saturdays – Sundays).

Select the Enable Internet usage blocking> select Block weekdays or weekends> select which hours of the day Check the Limit usage on the selected day’s box.

In the following image, user Administrator has been allowed internet usage only at 10-11 A.M on weekdays, and 9-10 A.M on weekdays. Thus, the user will spend on the internet 2 hours at the specified time interval on weekdays and weekends.

Computer Usage

Similar to Internet usage, user can define and control how much computer usage is allowed to a particular user on which day and at what time. Different settings can be chosen for different users.
LIVE UPDATE

Everyday frequent threat definition are released. Click on Live Update button to stay updated and protected with new malware.

Update from Internet

If you are online, let this option be selected, click Update Now button will download updates on your PC from the Internet website. This is manual update. This software is configured to also do automatically download updates.
Update from Intranet (Network path)

Click on ... Browse button available to select path on your PC or network path. From any PC where you have updated Max Total Security, go to C:\MaxAVLiveupdate folder and share this location when you browse or copy this on your desktop.

Note: Please browse only MaxAVLiveUpdate folder for local update from Intranet.

- When Automatic Live Update option from Settings menu is OFF and if new updates are available, you will be notified by a pop-up from your system tray once a day to do live update.
- If you do not want this reminder, you can turn it OFF by un-checking the Settings > Live Update Reminder option.

Offline Update

If you have internet on another PC or device then you can download and copy updates to your desktop and simply run the executable. You can browse this page to fetch downloads and update on any PC http://maxsecureantivirus.com/newdownloadupdates.asp .
Launch Support menu from the main interface.

This window contains the detailed information about your Registration details and various ways in which you can contact support, get registered, send logs, renew and register for laptop tracker.

- User first & last name as entered on the registration form
- Registration Number of the product.
- Subscription Expiry Date.
- For any Help Max Secure Toll Free Numbers, Live chat, Remote Support, Renewal information, email support
- Register for Laptop Tracker.
LAPTOP TRACKER

Lap Top Tracker is a service that works to track your lost or missing laptop.

Why Laptop Tracker?

- In coffee shops, college campuses, hotel lobbies and vehicles, laptop and notebook computers are being targeted by criminals at an alarming rate. You could just accidentally leave it in a restaurant or a cab. According to the FBI, 97% of stolen laptop computers are never recovered.
- Laptop Tracker offers service for individuals to track, locate and help recover their stolen/lost laptop computers. This service can track it down to the street location and show exact location.

Features

Easy to Install & Use

Laptop Tracker is a very easy to use application. To get started, you need to create an account with a username and password from Support>Register for Lap Top Tracker.

Locate: Tracks and maps the location of your laptop

1-Click Web Activation

As soon as your device gets stolen/lost, you can log in to your web portal from any pc or mobile device, mark as stolen and start Tracking. You would start getting alerts in your inbox.

Exact Location

Laptop Tracker uses IP based positioning that transmits the location of your laptop.

- Fill the details present in the registration form and click on Register button.
Tell a Friend

Once you register your copy of Max Secure Total Security, You would notice **Tell a Friend** button. If you click on this button and follow the subsequent instructions, you can mail a friend about Max Secure Total Security.

Renew Now

Once product is registered, you would notice this button. From here you can top-up or add more registration keys to increase the validity and expiry date of this product. So even if you have let us say 200 days left to expire, you can add another key of 365 days so that now you will have 365+200 = 565 days to expire.

Live Chat

You can contact our Technical Support team 365x24x7 by clicking on **Live Chat** button and resolve issues very quickly.
Remote Support

- If you are experiencing any critical issue and need to resolve right away such malware issue or difficulty registering the product or update issues then support team can connect to your PC remotely and resolve issues in rapid mode, at no cost to you.
- You need to give support team on chat your ID and password so that they can connect to you as below:

![Max Secure QuickSupport](image)

Export Log

- This optional feature is suggested by Max Secure Technical Customer Support if users are having any particular threat related issues on their system. Clicking on the Export Log button emails Max Secure support Team all the logs for further analysis.
- These logs help Customer Support Team to help other customers. It also enables us to analyze the new, emerging threat and help User community.
Export Log

Export Log will export system log, it helps our support team to resolve your problem.

* Your Email ID:
Your email address is important for us, so that our Research team can review and get back to you.

Subject: Select the issues you are having from the list below:
Please choose one option

Comment: Please add your phone number along with comment so that we can call you.
If you have any additional comments, please write below:

Send Log  Cancel

If you have any questions, please contact the Max Secure Software technical tel@maxsecure.com

Send Log  Cancel

If you have any questions, please contact the Max Secure Software technical team at info@maxsecure.com
MAX SHIELD

Click on the Max Shield button on the main Max Secure Total Security window to view these features. Various Monitoring options are described below:

IE Home Page Protection

- Whenever any program attempts to change Internet Explorer home page settings, Max Secure Total Security's Home Page Protection displays a message "Your home page is being changed to <url> (for example http://www.abc.com) do you want to do this?"
- If you click on OK, it will allow the home page to be changed. If you click Cancel, it will prevent home page from being changed.
- It is recommended that you keep IE Home Page Protection turned ON.

Tracking Cookie Protection
• Spyware programs install spyware cookies or Tracking cookies on your PC without your permission. When you surf websites on the internet, tracking cookies can capture your browser information, your IP address and other such details.
• With "Tracking Cookie protection" turned ON, whenever you open any website that attempts to access the third party or tracking cookies, these tracking cookies are deleted immediately. Thus the website(s) cannot access information about your system.
• This keeps your browsing habits, IP address, searches, preferences etc. private

Active Monitor

• Active Monitor provides immediate protection against malicious threats to your PC, it does not let any intruder get on your PC, terminated immediately even before they can land on your PC.
• Keep Active Monitor ON to keep system safe from online threats.

System File Protection

• This is a protection component designed to monitor a computer vital locations such as system 32, windows protected.
• If you are installing a software or doing Windows update, you can turn off System File Protection as once this option is ON no file modifications are allowed in those folders.

Note: By default this option is set to OFF.

Network Monitor

• Many spyware establish connection with their remote servers to send information.
• Network Monitor continuously monitors network activities for suspicious Network connections.
• If any Suspicious Network connection is found then this connection is closed by the Network Monitor and the process which was establishing this connection is also terminated.
• User is notified with a message “Suspicious Network connection was established to the <IP address> IP Address. Max Secure Total Security has terminated the connection.”

File Association Monitor
Windows operating system keeps a track of application to file extension association. For example a file with .txt extension will open by default by notepad.

- If this protection is ON, warning message is displayed when you try to change the extension of the file.
- On the warning message, If user selects "Yes" it will be allowed and if selected "No" it will be blocked.

Windows Restrictions Monitor

- Windows Restrictions Monitor protects your PC from many Window settings related changes made by any program.
- Many Spyware would create restrictions such as
  
a) Disable/Enable Drives  
b) Disable Control panel  
c) Disable Change Password  
d) Disable Search  
e) Disable RUN  
f) Disable Shut Down  
g) Disable Network Access  
h) Disable Taskbar Setting  
i) Disable RegEdit  
j) Disable Task Manager  
k) Disable Context Menu  
l) Disable Desktop icon  
m) Disable Display Properties  
n) Disable Background Tab  
o) Disable Screen Saver Tab  
p) Disable Setting and Plus Tab  
q) Disable Appearance Tab

Spyware exploit these registry entries. If some program tries to change these settings then Windows Restrictions monitor prompts the user whether he wants to allow these changes and blocks changes until input from user is received. User can make a decision if he is installing some program then he can allow otherwise he should say No.
IE Restrictions Monitor

Many Spyware manipulate Internet explorer to force users to go to their advertised websites, redirect searches, change homepage, popups etc.

Internet Explorer Restrictions Monitor protects your PC from changes in your Internet Explorer registry settings such as:

a) NoFileOpen
b) NoFileNew
c) NoBrowserSaveAs
d) NoBrowserOptions
e) NoFavorites
f) NoSelectDownloadDir
g) NoBrowserContextMenu and more

If some program tries to change these settings then it asks the user whether he wants to allow these changes. To allow changes click ‘Yes’ otherwise click ‘No’.

Enable/Disable the Active Protection

To Enable / Disable Active Protection you can do right click on system tray Max Total Security shield icon. You can do the same from here also. Options to choose are:

a) Enable after 15 minutes.
b) Enable after 30 minutes.
c) Enable after 1 hour.
d) Enable after next reboot

Please Note: If you disable Active Protection, your PC can get infected with trojans and viruses.
Max Secure Total Security

If you disable active protection, your PC can get infected with Trojans and viruses. Max Secure Total Security can no longer protect your PC with live monitoring; leaving it exposed to the latest security threats.

Select Action:
- Enable after 15 minutes
- Enable after 15 minutes
- Enable after 30 minutes
- Enable after 1 hour
- Enable after next reboot

Cancel
SETTINGS

Settings button allow you to customize many usability features based on your preference. The settings tab has two sections - Custom Settings and Advanced Settings.

Custom Settings

Following are the options in this section:

a) **Show live monitoring system tray notification:**
   Un-Checking this option will stop giving you pop up messages whenever Max Secure Total Security finds/quarantines any threats.

b) **Clean Temp/ Recycle Bin Files:**
   After you quarantine the threat detected by Max Secure Total Security, it also deletes all the files from the temp folder. It is recommended to keep this option checked as there are many threat, which keep their files and executables in the Temp folder.

c) **Clean Temporary Internet Files:**
   This option will let Max Secure Total Security delete Temporary Internet files after every quarantine. It is recommended to keep this option checked as many Malware programs keep
their executables in this folder.

d) **Show Tips at startup:**
Checking this option will show you the Tips window whenever you open Max Secure Total Security.

e) **Show splash screen:**
Checking this option will show you the Max Secure Total Security Splash screen whenever you reboot the PC, notifying you that your system is protected by Max Secure Total Security.

f) **Automatic Live Update:**
Checking this option will automatically check for the live updates at each start up and download them if they are available. If this option is unchecked you need to do live updates manually by clicking on the Live Update button on the main interface of the product.

g) **Live Update Reminder:**
Checking this option will show you Live Update reminder only if Automatic Live Update option is OFF. If this option is unchecked, you will not see any update reminder messages.

h) **Enable Sound Effect:**
Checking this option will play a Sound after completion of scanning and cleaning of threats.

i) **Do not take quarantine backup:**
Check this option if you don’t want to take backup of the malware files deleted/repaired by Max Secure Total Security. If you check this option you will not be able to recover the cleaned/repaired samples if you ever decide to restore your original file.

j) **Show Gadget:**
Checking this option will show Max Secure Total Security Gadget on desktop for easy access to scan, update and settings.

**Advance Settings**
Following are the options in this section:

a) **Generic Keylogger Scan**: Checking this option will scan your PC for detection of generic keyloggers.

b) **Start scan when Windows start**: Checking this option will automatically schedule the Max Secure Total Security to start scanning the PC every time you restart your computer.

c) **Clean the Rootkits**:
Checking this option will allow you to clean the rootkits. To enable rootkit cleaning for one time, select 'One Time Only'. You can also select 'Always' to enable rootkit cleaning option for every clean.

d) **Participate in Threat Community**:
Checking this option, user can participate in the Max Secure Threat Research Community. Threat Community program scans your PC once in a day, at low priority in the background, to detect for any new and un-identified threats and sends any suspicious data to Max Secure server for analysis.
e) **Enable Auto Clean:**
Checking this option, all threats detected will clean automatically and threat entries will directly move to the recover window.

f) **Enable Gaming Mode:**
Checking this option, will enable the Gaming mode, where you can play games or software using heavy resources.

g) **Protect system registry:**
Checking this option gives protection to some registry values like userinit, shell etc. so malware unable to change these registry values.

h) **Enable On copy Protection:**
This option gives On copy protection from malware. When you copy malware samples on your system it will catch them as soon as you copy them.

i) **Block Replication pattern:**
By checking this option, Trojans which replicates themselves will be blocked.

j) **Enable Log On Screen:**
Show the Logo of Max secure Total Security on windows logon screen.

   **Note:** This Option is available only for Windows XP.

k) **Enable Auto Clean:**
Keeping this option ON will automatically quarantine/delete/repair malware files as soon as they are detected by Active Monitor or Scheduled or on demand Scan.
Proxy Settings

Checking this option will allow user to configure proxy settings which will be used by live updates to connect to the Internet.

Scan By Name

- This option lets you add any file that you think is infected. The added files will be deleted from your PC and moved to quarantine folder. Very useful feature, used mostly by advanced users or Support team.
- You can add any file in **Scan by Name** window through Browse button provided beside the edit box and click on Add button. Then our scanner will scan those file, when you do any type of scan from all the locations of your PC.
a) Before adding file to Scan by name list, click on browse button or manually enter path of that file on textbox.

b) After browse or entering file path. Click on Add button to add file in list.

c) If you want to remove some file(s) from list. Select that file from given checkbox in front of the file. Click on Remove button to remove that file in list.

d) Click on OK button to save changes you have made in list.

e) Click on Cancel button if you do not want to save changes you have made.

f) Start scan to scan /quarantine the files in this list along with the other files on PC.

Notes: File you have entered in the list will be scanned and deleted if found anywhere on the PC. Do not enter legitimate files in the list.
Product Info

Click on the Product Info tab to view all the version information and when last Live update was done on your PC:
OPTIONS

This section contains many useful features mostly meant for people who want to do more than scan their PC and understand windows PC system and Windows registry and manage their processes on their PC for better optimized usage.

Exclude–Recover

With the help of this option, user can select the threat by name or by particular entry or the folder that he/she doesn't want to be scanned by Max Secure Total Security, can be added from here. If you want to start scanning this folder again you will have to remove it from this list.

Exclude

With the help of this option, user can select the scanned threat by name or by particular entry that he/she doesn't want to be scanned by Max Secure Total Security.

a) Scanned Threats List displays all the threat name and scanned entry path on your PC it detected during the last scan. You can select any threat name or particular threat entry that you’d like to exclude by checking the checkbox(es) provided before the threat name(s) or entry. The 'Select all' button lets you select all the threat in the list at one go.

b) Click the Exclude button to exclude the selected threat from the next scan.
c) These excluded threat or particular entry will not be scanned next time.

d) The excluded threat can be scanned again if you later decide to do so by clicking on the Recover button. As before, select the threat Name or entry you’d like to recover before clicking on Recover button.

e) Excluded Threats and Folders List consists of threat / folder that you have chosen to exclude from scans.

f) Select the entries that you want to be scanned and click on Recover.

g) Next time when you scan the PC, these threat / folder will be scanned

**Cookies /BHO**

**Cookies**

This option lets you delete any cookies and Browser Help Objects (BHOs) from your system. You can view this section by clicking on the Cookies BHO tab of the Options window.

Select the checkbox (es) next to the cookie(s) you wish to delete in the list and click the Delete button to perform this action. If the cookie(s) was (were) successfully deleted, Max Secure Total Security will display a confirmation window saying, "Cookies deleted successfully". Click OK to return to the previous window.
BHO

Many BHOs (Browser Helper Objects) may have been installed on your PC without your prior permission. Such objects may or may not be helpful.

a) The BHO section displays a list of BHOs that Max Secure Total Security found on your PC. You can choose to block any BHO found in the list. Blocking prevents the BHO from running.

b) Select the BHO you want to block and click on Block.

c) When you click on a previously blocked BHO, notice that the Block button changes to Unblock.

d) You may select the BHO and click on Unblock to allow the BHO to function again.

e) The Export button lets you save the list of BHOs into a text file. Click on that button and follow the subsequent instructions.
Recover

After cleaning threats found during a scan, you can either delete these malicious programs or recover them out of quarantine vault, if you need them. Normal usage of the Max Total security does not require you to do anything but if you want to delete the quarantine data or restore deleted files then you would use this feature.

Click on Recover button in the Options Window and you will see all of the threats that you had cleaned so far. Your PC is safe and isolated from these threats. Recovering them will result in all the threats becoming active again and your PC will become infected. So recover with caution.

This option helps you Recover or Delete these programs that have been isolated. The Recover option has been provided in case you actually need any of the isolated programs, or if any associated program stops working due to the clean process.

You will notice five buttons on this window.

1. Load List
2. Recover & Exclude
3. Recover
4. Delete
5. Cancel

To start using Recover option, first click on Load List button.
a) To recover any threat entry and do not want Max Secure Total Security to scan it again, click on Recover & Exclude.

b) Only to Recover the threat and restore them to where they were originally placed, click on Recover.

c) To permanently remove these deleted files from your PC, click on Delete. After clicking on Delete you will get a message window of Warning, that if you delete these entries then afterwards you will not be able to recover these entries again. To do nothing with cleaned threat, click on Cancel.
Notes:
When product has cleaned threats, they are already deleted from your PC, your PC is safe now and deleted threats are moved to vault. Threats deleted using the Delete option here permanently removes them from vault and cannot be recovered later.

Registry / Hosts File

Spyware programs perform such malicious operations by changing some settings in your Windows Registry. This section lists all the settings in the Registry that Max Secure Total Security has found to be changed.

You can select any or all of the settings that you want to fix and hit the Fix button. These settings will be restored to their original default values as set by Microsoft Windows during the installation of the operating system.

You may change these settings manually in the Registry at any time without any interference from Max Secure Total Security. Note that this option is to be considered a rescue option when spyware programs disable many normal operations on your PC and browser.
Hosts File

Hosts file contains mappings for domain Names/IP address to IP Addresses. Spyware or hijackers use this file to block any website from opening in browser and redirect them to site of their interest. We continuously monitor the Hosts file for any access by any program.

Hosts file option allows you to insert and delete hosts name's from the Hosts file. You can delete any legitimate host name present in the file by clicking on the Delete button or you can add the any new spyware host name by clicking on the Insert button. When you click on the Insert button, you will get dialog box shown as below with the 2 edit boxes for IP Address and Host Name.

Please Note:
1) The IP Address and Host Name should point to the same web site.
2) Please do not add any legitimate web site, as you will not be able to browse that web site which is added in the list, so be careful.
Net Fix

Note: This option is recommended only for advanced users. By fixing registry settings, you may sometimes change any custom settings that you would like to retain.

- A Layered Service Provider (LSP) is a system driver linked deep into the networking services of Windows. It has access to every piece of data entering and leaving the computer, as well as the ability to modify this data.
- A few LSPs are necessary to allow Windows to connect your computer to other computers, including the Internet. But spyware programs may also install themselves as LSPs, thus having access to all the data you transmit. Some known spyware programs that use this method to access data are CommonName, New.Net, NewtKnows, and WebHancer agents. Such buggy or improperly configured LSP software can result in Internet connection problems.
- Max Secure Total Security displays a list of installed network drivers on your PC. If you want to fix Internet problems on your PC, click on the Fix Internet button. This will restore to your PC the original list of LSPs that were installed during your operating system's installation. Any LSPs installed by users or programs since then will be removed.
- If you want to export the list to a file for future reference, click on Export. In the window that opens, select the name and location of the text file that you wish to save the list in and click OK. The list will be saved in that location with that name.

Warning: Use this option only if you have Internet connection or network problems. If you use this option without any purpose, some valid applications using LSPs may stop working properly.
Process / TCP View

Process Entries

- Click on the **Process Entries** tab on the Process TCP View UI to see a list of currently running processes and their Process ID.
Max Secure Total Security allows you to terminate (Kill) some processes in the list. You can terminate any process by selecting that process's row in the list and clicking on the Terminate button.

To generate a text file list of these processes, click on the Export button. Follow the prompts that are displayed and the list of processes will get saved into a text file designated by you. Note: It is recommended that only advanced users use this option. Unnecessary termination of processes may lead to system instability and improper functioning of your computer.

TCP View

Click on the TCP View tab on the Process TCP View UI to see a list of currently established Network connections on your PC.

You get the information i.e. Process Name, Process ID, Protocol Name, Local IP Address, Local Port, Remote IP Address, Remote Port and Connection State of the established connection.

NOTE: This option is right now available only for Windows XP SP2 and later.
Max Secure Total Security allows you to disable (and enable) items in the list, as well as delete them, change them or insert new items. On Windows 95, 98 and Window ME systems, the user has full access to this list. On Windows NT/2000/XP systems, the list will display the global and the current user entries. For some functions like viewing all entries or even changing some, you may need admin or power user rights.

If you want to change any entry, select that item and click on Change. A box will appear that will allow you to change the value of the path to the executable of that program.

If you want to insert any new item in the startup list, i.e., add a program to the list so that it starts up with Windows, click on Insert.

A window will appear in which you need to specify the following values to create a new Startup item:

1. Root key - You can choose to create this startup item either for the current user only or for all users. If the former, this program will be started up only when the current user logs in. If the latter, this program will be started up for all users who log into this system.
2. Key - This specifies whether the program to be started up is a normal program or a service program.
3. Name - The name of the program to be started up.
4. Link of the item you want to insert - The path to the program executable.
   - When you restart your PC, that item will start at Windows startup, if you want to delete some item from startup list, select that item and click on Delete.
   - The next time you start your PC, this program will not start up along with Windows. Always use the Delete option with caution.
   - You can also export the startup items list to any place in a text file format by clicking on Export. Follow the prompts to specify the name of the text file that the information will be saved in as well as its location.
TOOLS

USB Manager

Steps to Enable USB Manager:
Click on USB Manager Button present in Tools option.

Set / Reset Password Protection:
When you set the password in Set / Reset Password Protection section then as soon as you attaches a removable device to the PC; it will ask for password to open Removable Device Scan window. If you want to remove Password then click on Remove Password button.

Scan Removable Devices:
Checking this option will scan removable devices which user attached to the PC. Manual: On selecting this option, any time a removable device is attached to the PC, a popup window will open with options - Scan and Cancel. Clicking on Scan would scan the removable devices only.
Auto: On checking this option, any time a removable device is attached to the PC, Max Secure Total Security will start scanning. This will only scan the removable devices.

Total Block

This is a very useful feature. These days data protection is very important where anyone can connect USB to your PC or company PC and download all the information on the drive and take away. This unauthorized access is now manageable using a password. This feature can totally secure your PC from unwanted programs running on your PC from USB device.

Autorun.inf

- The AutoRun function in Windows can launch installers and other programs automatically when you insert a CD or flash drive, but this convenience poses a serious security risk. Every recent version of Windows has features known as AutoPlay and AutoRun.

- These functions are designed to launch applications automatically from an external device containing the necessary AutoRun information. This is what causes an installer window to pop up when you insert a software disc into your CD or DVD drive, for example, or makes a pop-up menu icon appear in the taskbar tray when you insert a USB flash drive.

Read

If you want to make USB device not readable check Read checkbox.

Write

If you want to make USB device not writeable check Write checkbox.

Execute

- If you want to block execution of file from your USB device you can check Execute checkbox to block execution.

- However convenient this might be, unfortunately, AutoRun also opens a huge door for viruses, Trojan horses, and worms. All it takes is a USB flash drive with an autorun.inf file and an executable in its root. Once inserted, a worm launched in this manner can infect every disk partition it finds, jumping from computer to computer as network users connect to an
infected drive.

- USB Manager allows you to block AutoRun automatically so that you have control over when contents of USB drive run on your PC or not.

**Browser Fix**

- This tool used for resetting browser to original state.
- Click on Start > All programs > Max Internet Security > Tools > Browser Fix.
- Click on Remove toolbar button. This will remove all toolbars & extension from Firefox, chrome, Internet explorer, & opera mini. Please close browsers before you proceed.
- Click on Full Reset button. It will reset Firefox, Chrome, Internet explorer, & Opera mini completely. This will remove save Password, Cookies, Cache, Toolbars, Bookmarks, all your setting

NOTE: Please close the browsers before you proceed.
Max Live Update Fix

Tool to fix issue if you have Internet and still experiencing live update error, it could be due to Malware have infected your host file or redirecting maxpcsecure.com website to another IP address.

- Click on Start > All programs > Max Total Security > Tools > Live update Fix.
- Click on OK button. It will remove problem of not getting live update.
Max IExplore Fix

This tool scans and removes complex malware infection from your computer.

- Click on Start > All programs > Max Total Security > Tools > Max IE explorer Fix.
- Click on scan button. It will scan your system and clean complex malware.
- Click on cancel button to close UI.
Registry Backup

Max Registry Backup for Windows XP 32/64 bit

Create Backup
Your backup folder will be stored at location:
C:\WINDOWS\MaxSecureBackup

Start Backup

Restore / Delete Registry Backup

<table>
<thead>
<tr>
<th>Name</th>
<th>Creation Date</th>
</tr>
</thead>
</table>

- ○ Restore Backup
- ○ Delete Backup

Start

OK Cancel
Registry Fix

Some malware disable your system’s applications like task manager, Registry editor etc. to enable them you can use this tool.

- Click on Start > All programs > Max Total Security > Tools > Max Registry Fix.
- Check checkbox you want to enable and click on fix button.

Max Services List

Tool to see all the services on your pc. If you find any service to be suspicious then you can stop it from here conveniently using this tool and prevent malicious infection.

- Click on Start > All programs > Max Total Security > Tools > Max services List.
- Select service from list.
- Change start up type to disable if you are sure that service is malicious
- Click on save button.
Max System Volume Information Cleaner

Sometimes virus files may reside there and take unnecessary space and are hard to remove. This tool will completely clean that folder and also create a new Restore point for you in case, in future you may have to restore your PC.

- Click on Start > All programs > Max Total Security > Tools > Max system volume information cleaner.
- Click on OK button to clean all System Volume Information folder from all drives on your PC.
- Click cancel button to close tool.
Max Secure System Volume Information Cleaner

When to Use this Tool:

The System volume information folder can contain many virus-infected and unwanted files taking up space on your hard disk and making it susceptible to virus infections.

This tool will delete all the files from this location and also create a new restore point for you.

Press Ok to Start, Cancel to Quit

[Images of two success dialogs showing "Cleaned Successfully creating Restore Point..." and "Restore Point Created Successfully..."]
Security Vulnerability Scan

Vulnerability scan is a special tool which helps to search and eliminate security vulnerabilities of applications and operating system settings.
Max Rootkit Scanner

This tool scans and cleans your system from complex rootkit and complex spyware threats.

- Click on Start > All programs > Max Total Security > Tools > Max Rootkit scanner.
- Select drives and option by checking checkbox.
- Click on scan button to scan your system.
- After scan click on clean button to clean threads.
How to Create System Restore Point?

System Restore works a lot like the Undo command in Microsoft Word. You can use System Restore to remove any system changes. Windows creates restore points at the time of significant system events (such as when an application or driver is installed) or you can create and name your own restore points at any time.

When you run System Restore, a calendar is displayed to help you find restore points. You can go back to the time Max Secure Total Security installed from the label on Restore point list “Installed Max Secure Total Security” and click Next button.
Click on **Start > All Programs > Accessories > System Tools > System Restore**

**Max Un-Hide Folder**

- If due to virus/spyware you can’t see your data, and then use this tool to unhide hidden files/folders.
- Click on Max Total Security > Tools > Max UnHide Folder.
- Select path of folder by browse button.
- Click on Start button to unhide folder.
- Click on cancel button to close tool’s UI.
PC Tuner

Max PC Tuner tunes and Optimizes your PC Performance to give you fast and stable PC.

Max PC Tuner safely cleans repairs and optimizes Windows Registry, protects your privacy by removing all traces of internet and computer usage, turbo charges your Internet connection, frees up and defrags Physical Memory to make your PC running like new. This tool can also find duplicate files on your PC and you can delete them as per your preference to save space on PC. There are many features embedded in this tool and it is highly recommended to schedule it to run once every day. Detailed help is available on the program.
Safe Browser

Provides a secure way to browse. Steps to enable Safe Browser:

- Click on Safe Browser button present in Tools option.
- It will launch Safe browser which you can use to browse banking sites etc. It is recommended to use the virtual keyboard in addition to safe browser.
Virtual Keyboard

What is virtual Keyboard?

A virtual keyboard is a software component that allows a user to enter characters. A virtual keyboard can usually be operated with multiple input devices, which may include a touch screen, an actual keyboard and a computer mouse.

- Max Secure Total Security provides users a Virtual keyboard for keeping confidential information safe.
- To use virtual keyboard click on Virtual Keyboard button present on Main UI. After that virtual keyboard appears, use this to fill web forms or applications where you want to make sure that your data will not be stolen by some key logger program spying on your regular keyboard.
Max Data Backup Utility

This tool allows you to back up all of your document files automatically or manually on your PC. These files can be later restored in case you have accidentally removed some or all of them or they have been infected by some malware. Backup file are protected in a vault called “MaxSecureDataBackupTask” and can not be deleted from explorer view or infected by any malware. These files are compressed and intelligently backed up to optimize the space used by them.

They can be easily restored whenever user wants to with easy to use user interface. They can also be deleted using user interface if user is short of space. Convenient scheduler lets you backup files without your assistance although you can manually back them up as and when you like.

Back up comes with easy to find and search feature where you can search for backup file son various attributes such as name, date, month etc.

User is given a choice of minimum required file extensions but you can also select more and also add more extensions if you do not find them in the given list by us.
Data Backup Settings:

A. File Extensions: Different types of file extensions which will be backed up are displayed here.
   - **ADD BUTTON**: This button is used to add the new extensions.
   - **REMOVE BUTTON**: Remove button is used to remove the specific file extensions which are present in extension list.
   - **DEFAULT BUTTON**: This button is used to reset the extension list. It removes the newly added extensions and keeps only the default extensions provided by this tool.

B. Maximum backup size allowed (MB): It is used to fix the folder size in which the backup data is to be stored, default value is 600MB and user can increase the maximum backup size of the folder.

C. File modified within (days): It is used to take the backup of the file which is modified within the days which is selected from the drop down list, the default days is 60 and it can also be changed.

D. Maximum file size allowed (MB): It is used to fix the size of the file which is to be backup and large file should not be backup its skip the file.
E. Change backup drive: By default this program selects a drive with maximum space for back up but user can choose to change the drive for back up.

F. Daily: We can schedule to do daily backup, default is weekly.

G. Weekly: We can select the weekly check box where we can select the day from the drop down list to take backup on that day, we can also change the day to take backup.

H. Monthly: We can also select the monthly check box and the each month its will automatically take the backup.

- **SAVE BUTTON**: Saves the modified settings.
- **CANCEL BUTTON**: Cancel the changes.

**RESTORE BACKUP:**

RESTORE button is used to restore the data to its specific path, we can also change the path of storage by selecting from the restore path.  
We can search the backup data from selecting the options:
- Month
- Week
- Year

We can also directly search by:
- File name.
- Modify date.
- Extension.
MANAGE BACKUP: Manage backup button is used to manage the backup data, we can select the data and DELETE the data.
Shortcut Keys (Hot Keys)

For easy access to features, we have provided some Hotkeys or Shortcut Keys without the help of mouse. They are listed in the table below.

<table>
<thead>
<tr>
<th>Functions</th>
<th>Shortcut Keys (Hot Keys)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan</td>
<td>Alt + S</td>
</tr>
<tr>
<td>Clean</td>
<td>Alt + C</td>
</tr>
<tr>
<td>Export Log</td>
<td>Alt + E</td>
</tr>
<tr>
<td>Max Shield</td>
<td>Alt + M</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Alt + D</td>
</tr>
<tr>
<td>Options</td>
<td>Alt + O</td>
</tr>
<tr>
<td>Live Update</td>
<td>Alt + L</td>
</tr>
<tr>
<td>Register Now</td>
<td>Alt + N</td>
</tr>
<tr>
<td>Close Window</td>
<td>Alt + F4 or Alt + X</td>
</tr>
<tr>
<td>Protection Center</td>
<td>Alt + P</td>
</tr>
<tr>
<td>Support</td>
<td>Alt + U</td>
</tr>
<tr>
<td>Settings</td>
<td>Alt + I</td>
</tr>
<tr>
<td>Tools</td>
<td>Alt + T</td>
</tr>
</tbody>
</table>

Discussing on Forum

If any of your questions are not answered by our

Email experts (http://maxsecureantivirus.com/contact.htm),

Chat experts, Live chat button on http://maxsecureantivirus.com website,

Or Remote Desk Support at no cost to you, avail this opportunity by asking for Free remote desk top support from any of our chat experts if you have ANY issue such as registration, activation, malware, updates or installation, we will do it for free.

Then you can go to http://forum.maxsecureantivirus.com/ and discuss issues.
Blog for latest Security news and Product updates

You can read frequently updated useful News here http://blog.maxsecureantivirus.com/

Feedback

We highly regard your feedback and feel happy to receive positive or negative feedback, we are always trying to improve and you are the best critique. Please drop an email to http://maxsecureantivirus.com/contact.htm if any of your issues do not get resolved.

Useful links

Max Secure Anti-Virus Web site  http://maxsecureantivirus.com
Max Secure Forum  http://forum.maxsecureantivirus.com/
Max Secure blog  http://blog.maxsecureantivirus.com/
Help me choose right product for me  http://maxsecureantivirus.com/compare.htm