Protegent®

Total Security Solution

USER GUIDE

Table of Contents

PROTEGENT TOTAL SECURITY....3

INSTALLATION....4

REGISTERING PROTEGENT TOTAL SECURITY....10

WORKING WITH PROTEGENT TOTAL SECURITY....11

- SCAN....13
- USB....14
- WEB PROTECTION....15
  - Application Rules....16
  - Categories....17
  - Time Restriction Feature....18
  - Keyword Blocking....19
- SETTINGS....20
  - Protection....20
  - Scanner....21
  - Update....22
  - USB....23
  - Scheduler....24
  - Logs....25
  - Notifications....26
  - Password....27
  - License....28
- UPDATE....29
- LICENSE....30
- ABOUT....31
- LOGS....31
- QUARANTINE....32
- WHITELIST....33

UNINSTALLING PROTEGENT TOTAL SECURITY....34

PROTEGENT TOTAL SECURITY

USER MANUAL

Introduction:

Welcome to Protegent Total Security.

Protegent Total Security is a collection of high end technologies that work in perfect synergy, having one common goal: to protect your system & network and valuable data against computer viruses. It represents a superior solution for any Windows based workstation.

Protegent Total Security incorporates Total Security 360, Antispyware, Anti Malware & Anti-Rootkit technology. With firewall & sophisticated protection capabilities Total Security 360 ensures that your valuable data and programs are always protected.

This manual describes Protegent Total Security installation and operation. For further options and information, please visit our website:

www.protegent360.com

Protegent® Team

INSTALLATION

Before starting installation:

Make sure that no other virus protection solutions are installed.

The automatic protection functions of various security solutions may interfere with each other.

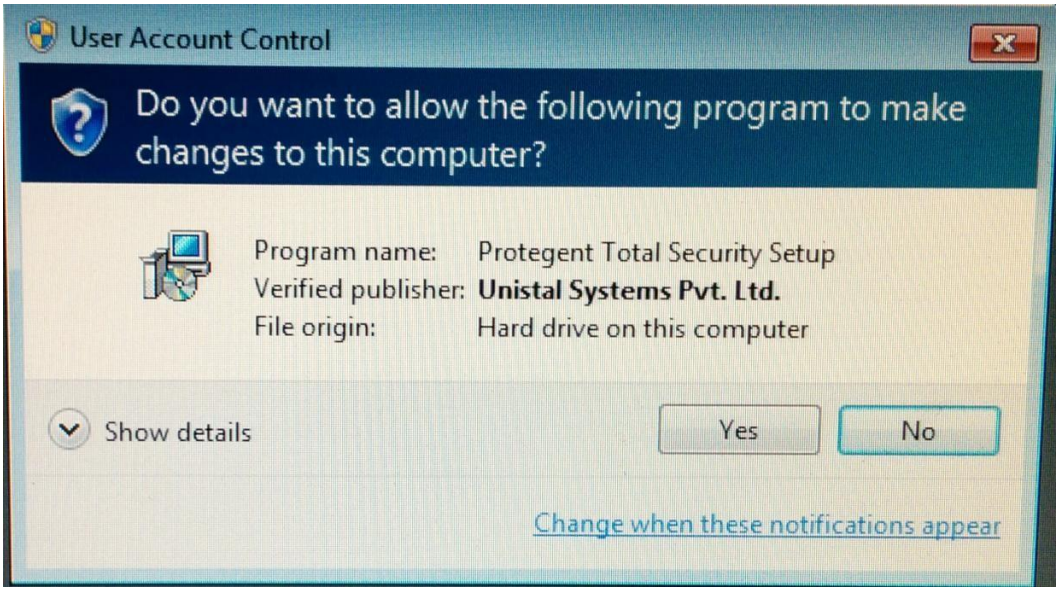
Install: The installation program runs in a self-explanatory dialog mode. Every window contains a certain selection of buttons to control the installation process.

The most important buttons are assigned the following functions:

Next	Go to next step
Back	Go to previous step
Install	To process installation
Finish	Action finished

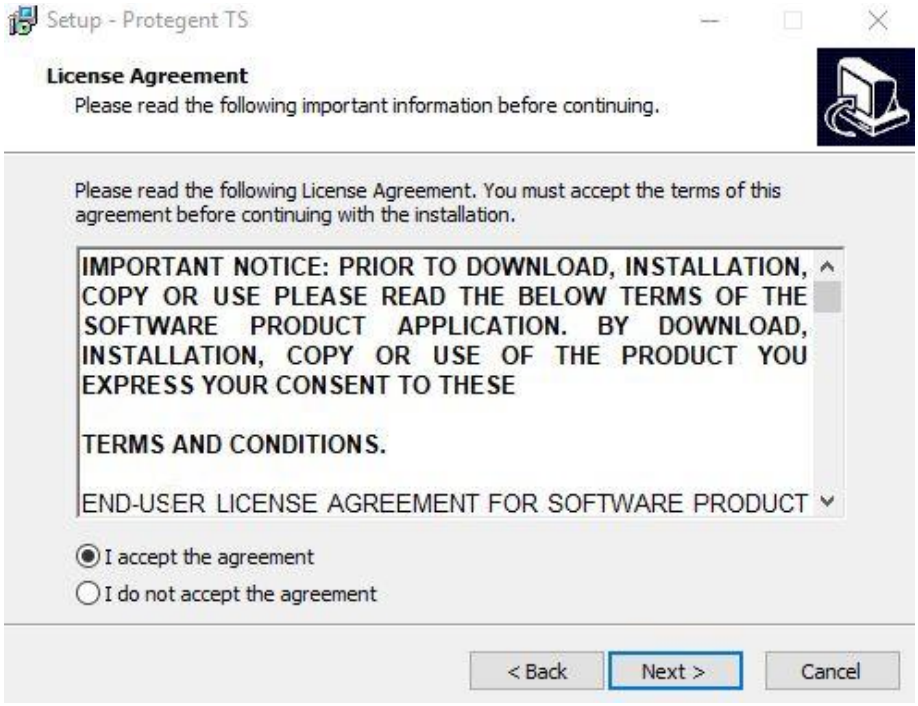
INSTALLING YOUR PROTEGENT TOTAL SECURITY

- Install by running the “ProtegentTS.exe” installation file by double clicking on it.
- Clicking “Yes” will take you to the Protegent Total Security Setup screen:



- Click “Next” and the installation Wizard will then guide you through the rest of the installation process.

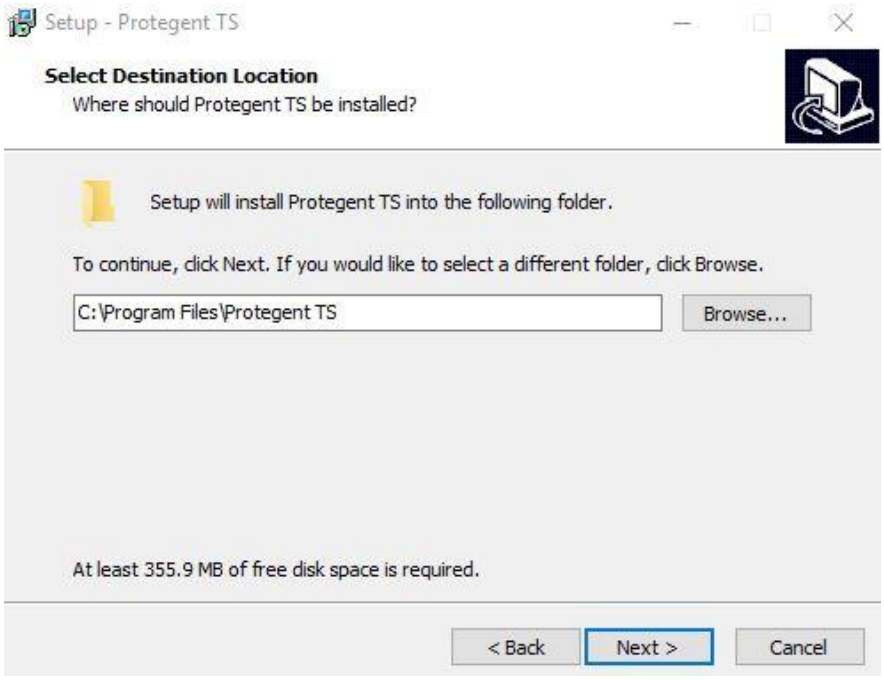
- First you will be asked to read about the minimum system requirements and then confirm that you to agree to the end-user license conditions.



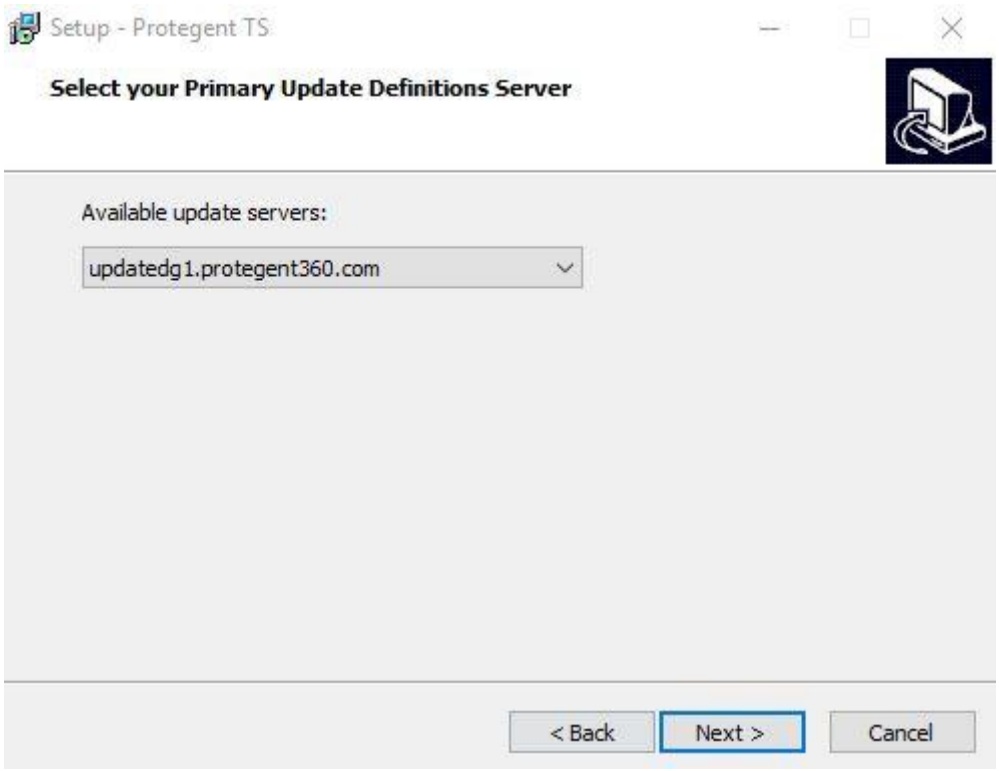
- To continue, click on "I accept the agreement", this enables "Next" for further steps.

- Clicking on "Next" will navigate you to the destination selection window.

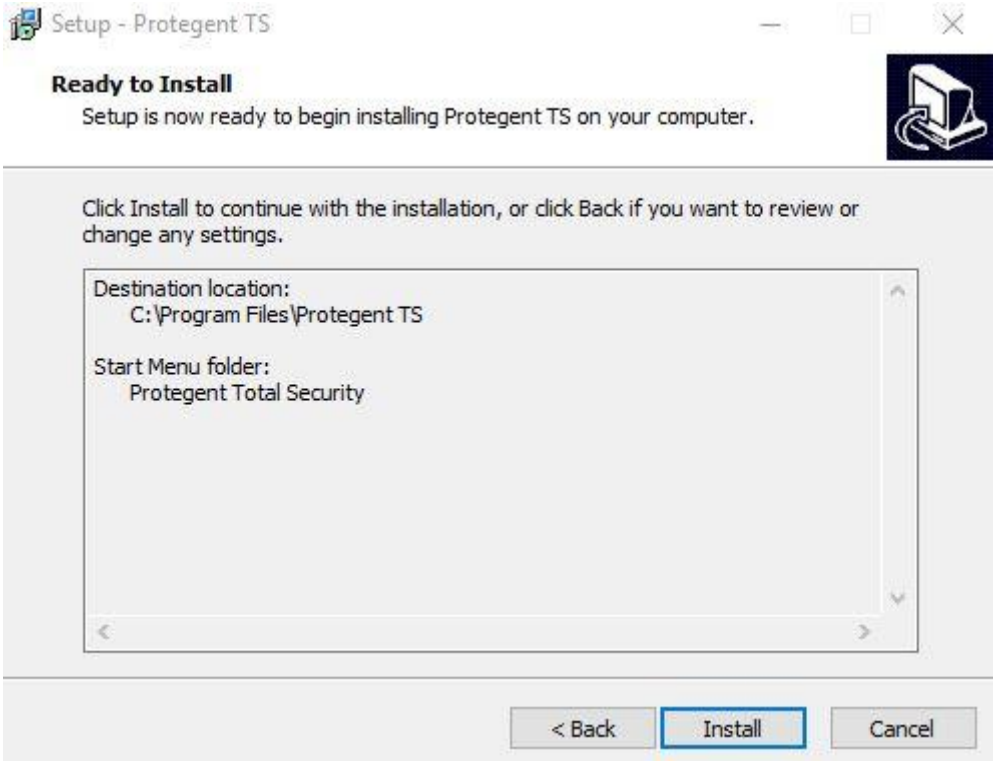
- You will be asked to confirm the destination directory, i.e. where the program files will be saved. The program will select this automatically or will create a new directory if it doesn't already exist. It is recommended to accept the default destination directory and simply click on "Next" to continue.



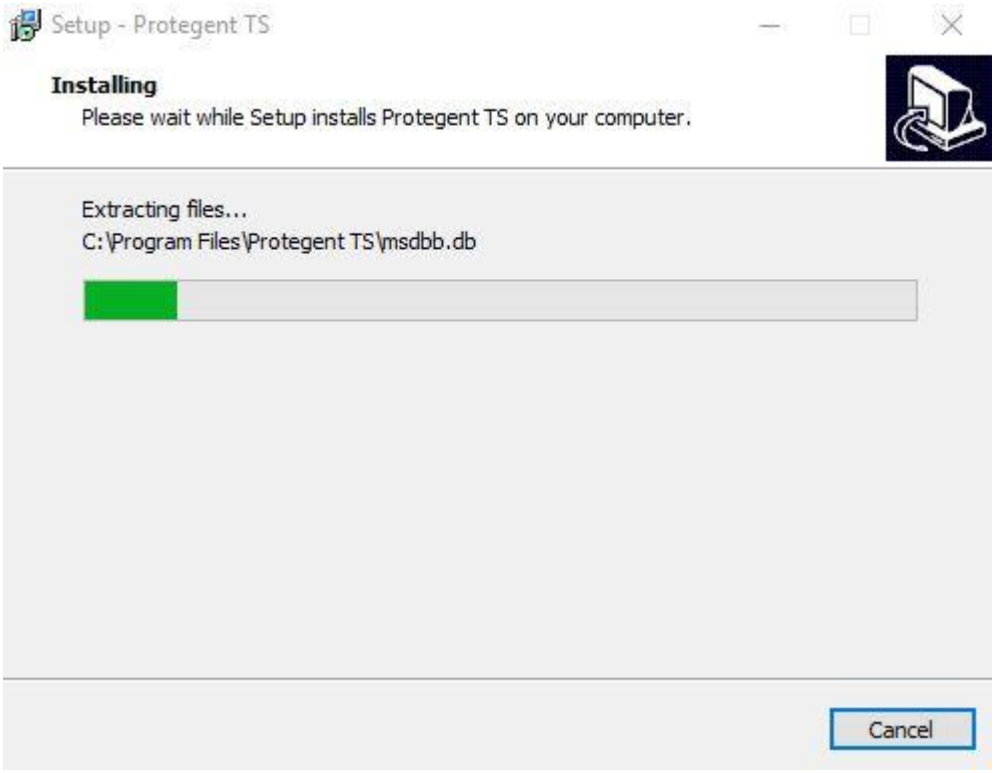
- ▯▯w selects your “updatedg1.protegent360.com” as Primary Update Definitions Sever.



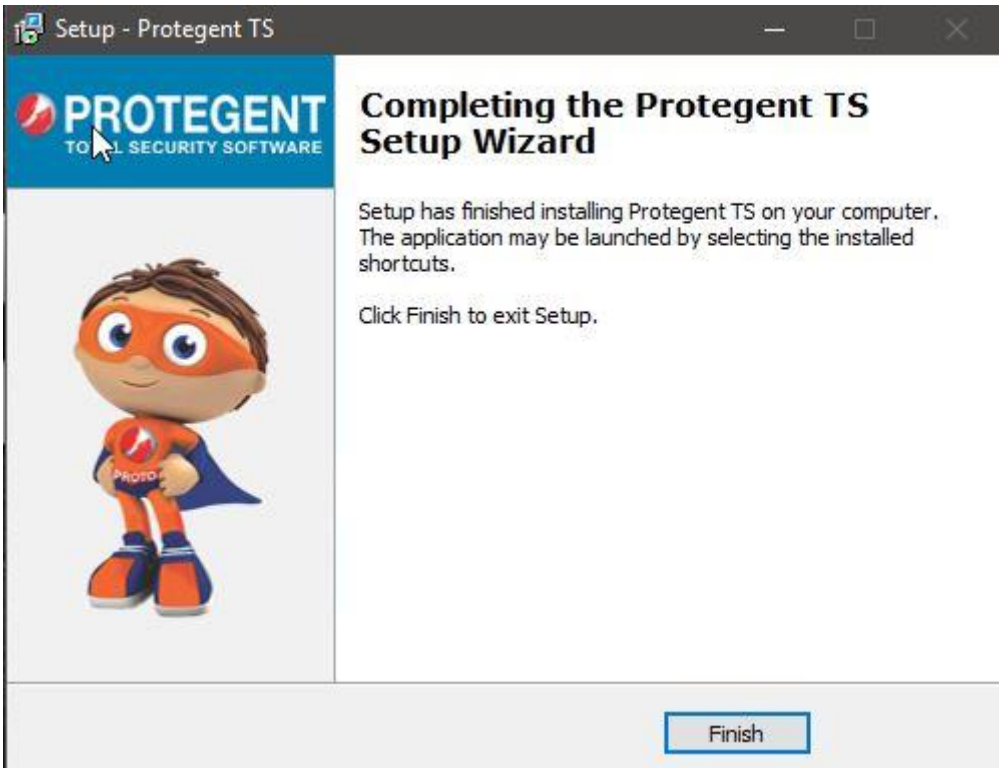
- Now the setup is ready to install the Protegent Total Security. Click on "Install" for the installation process.



- The installation progress will display as a green progression bar as shown in the screen below.



- Protegent mascot "**Proto**" on the left bar confirms that installation has been successfully completed and ensures you with the "Finish" setup wizard.

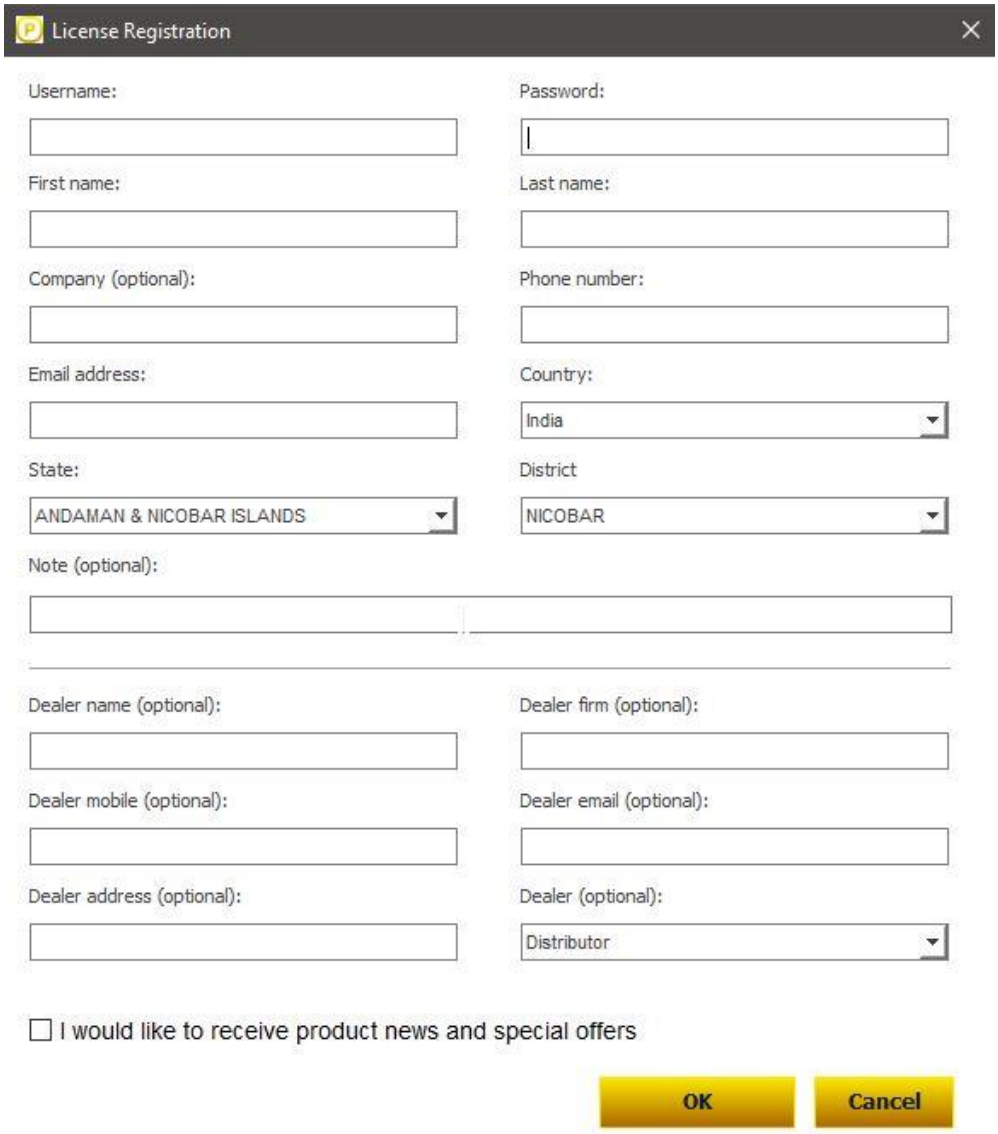


- Click on "Finish" to complete the process. With this the installation task has been completed.

- After installation is completed, Protegent Total Security will show a message of license expiration as follows:

REGISTERING PROTEGENT TOTAL SECURITY

- Please click on License button on the top right hand corner in order to register Protegent Total Security.
- It will display the License registration page as shown below.



- Copy and paste the license number under username tab and password in password tab accordingly.
- Then go ahead and fill-in the details and click on „ok" to complete the registrations process.

Once done it will activation your license accordingly.

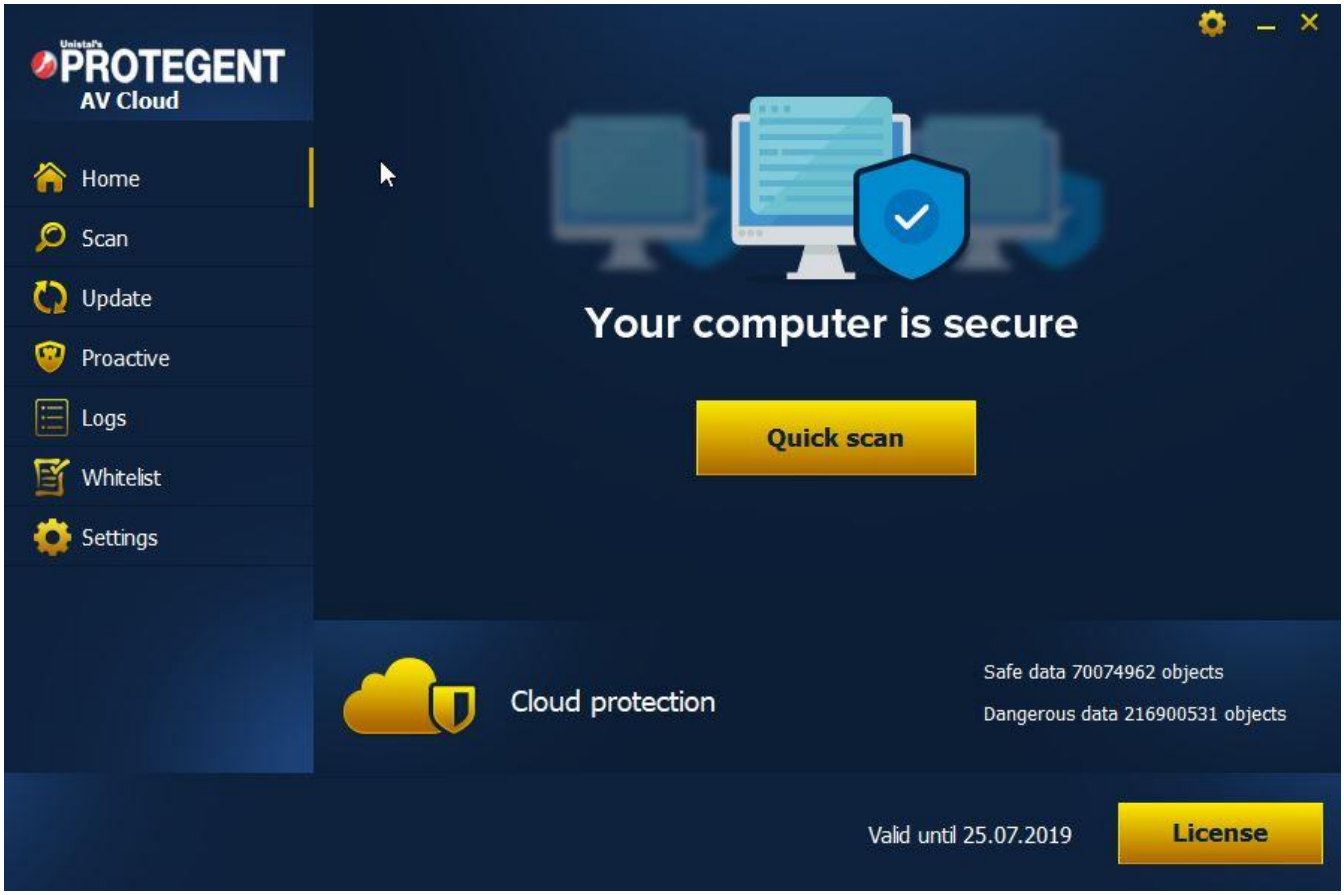
Please Note: Restart the system after installing "Protegent Total Security" in order to get the registry updated and work fine without any issues.

WORKING WITH PROTEGENT TOTAL SECURITY

After installation, a Protegent Total Security shortcut icon will appear in your taskbar. Click on the icon to see the details of Protegent Antivirus.

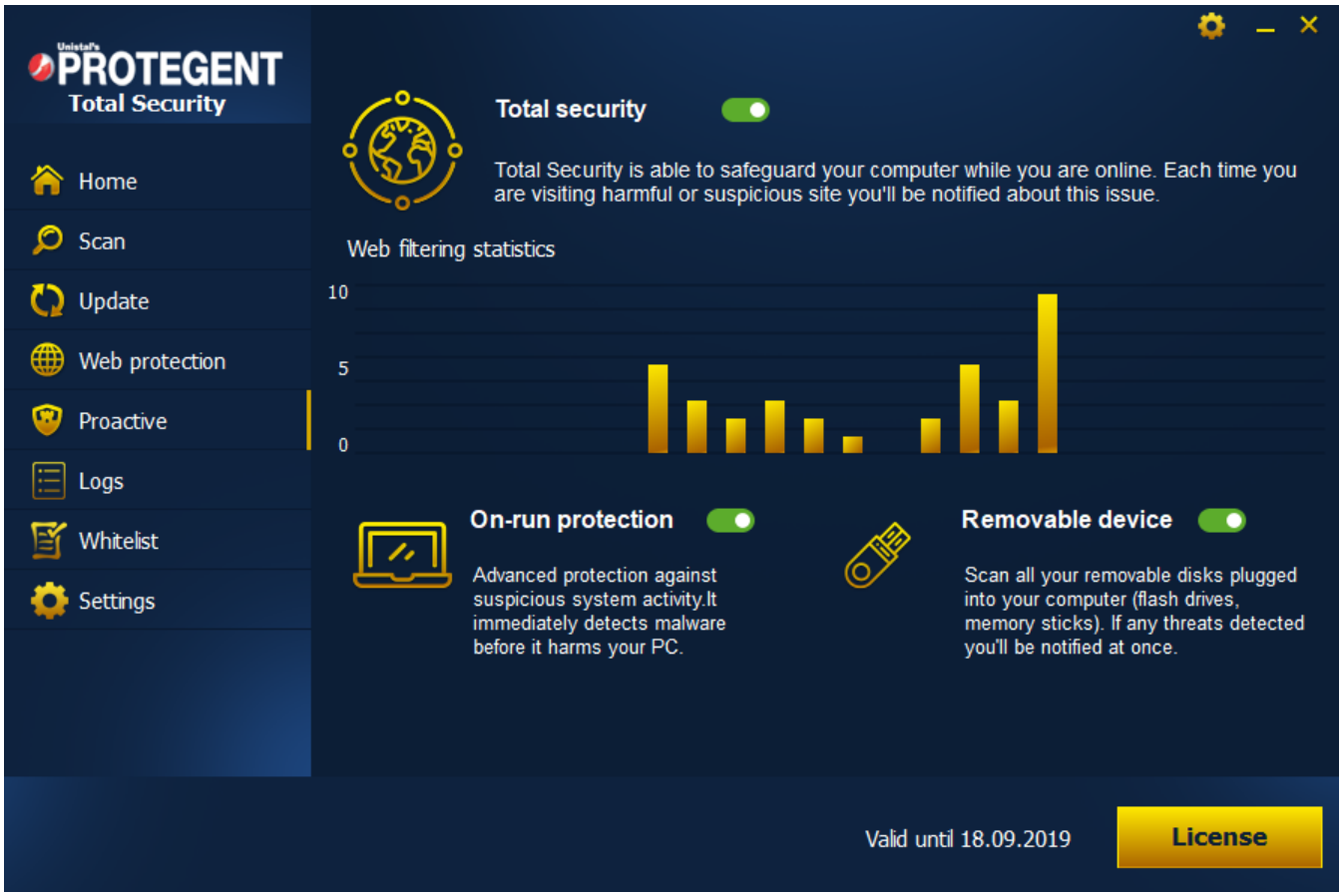
If you right click on that icon, it will show options to view the GUI, Update, and Real- time protection options as shown below.

When the user opens Protegent Total Security, the screen will appear like as below:



PROTEGENT TOTAL SECURITY OVERVIEW

The Protegent Total Security overview screen contains different options as shown below. Clicking on a screen will take you to that particular screen options.



SCAN

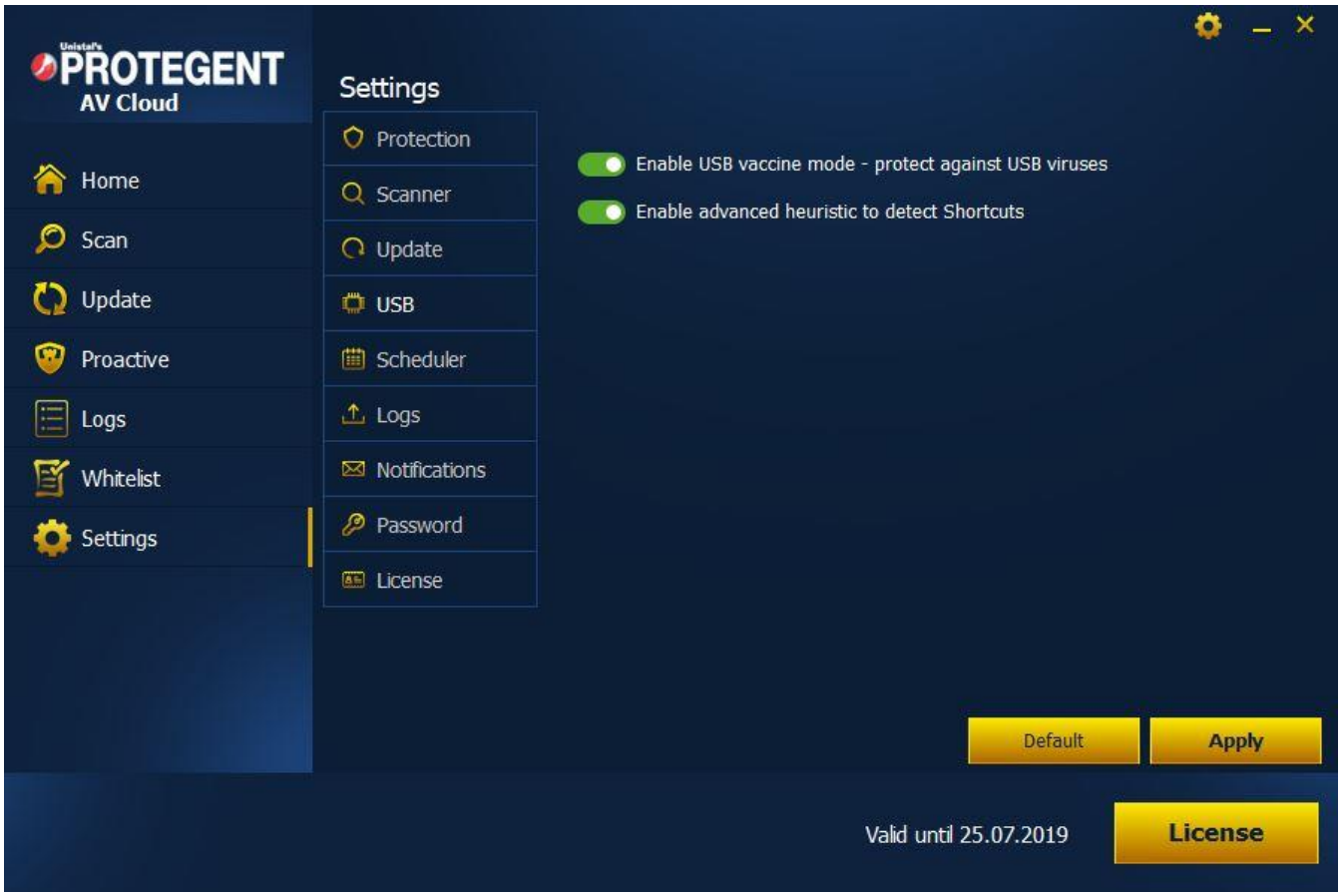
- If you want to run quick, full system scan, external devices or specific folders scan in your system then select the respective “Scan” option.

- Then select the scan option and click on “Scan Now”.

- You can also scan the files by right clicking on the file which gives you many options.

USB

- The USB tab shows an option of enabling vaccine mode which provides protection against USB viruses
- You can also enable advanced heuristic which detect any sort of shortcut viruses in USB and also enables protection from viruses for which virus definitions are not updated in the software.



WEB PROTECTION

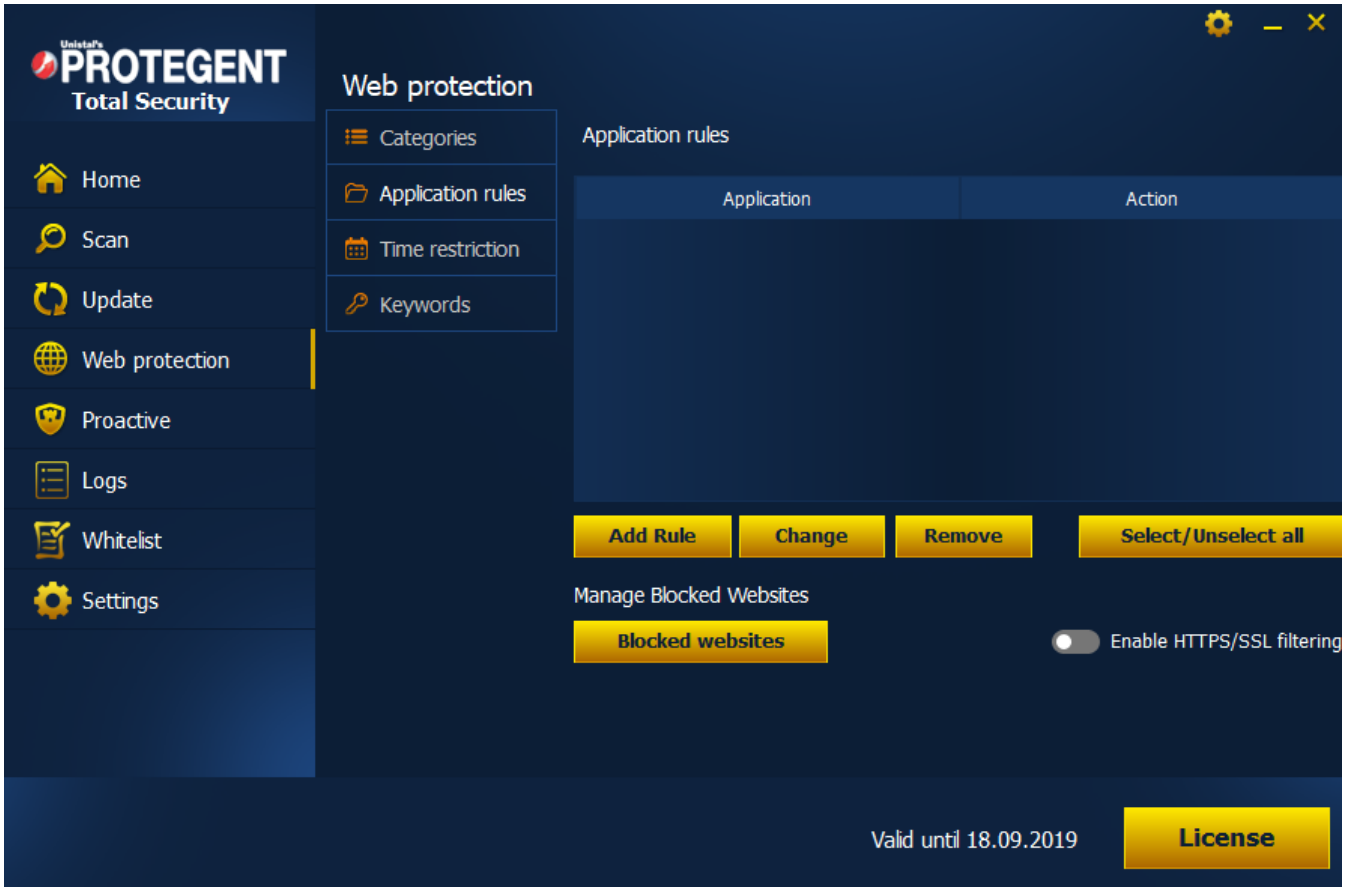
Web Protection can be setup using either Applications Rules, Categories, Time Restrictions and keywords.

- You can configure the Protegent® category from the application.
- In the application based URL categorization, each row represents one feature. You simply have to check or uncheck checkboxes to enable or disable the features under the Categories section.
- When a check box is checked, then that particular feature is enabled.
- This feature ensures Web applications are used exactly as intended in organizations. It protects against the manipulation of Web environment for malicious intentions and provides an added level of security by the application infrastructure. It has a strong defense against known and emerging hacking attacks and has optimal predefined security rules for instant protection.

Application Rules

Protegent® application Rules issued to block/restrict TCP/IP, UDP internet based traffic Protocols and application from being installed or executed. It will show as the application is loading/accessing but will restrict and display the results.

- Click “Application Rules” on the left-hand column menu under Firewall.
- Please Enable HTTPS/SSL filtering button and click on ADD RULES.
- Select the application from the location and click open. E.g.: Chrome/IE/Firefox or select the application from the location e.g - .exe or installation file.
- Select the .exe application from the location and click open e.g.skype.exe
- Select the option under custom rule as per need and click on apply.
- When we try to access the application it will display the message accordingly.

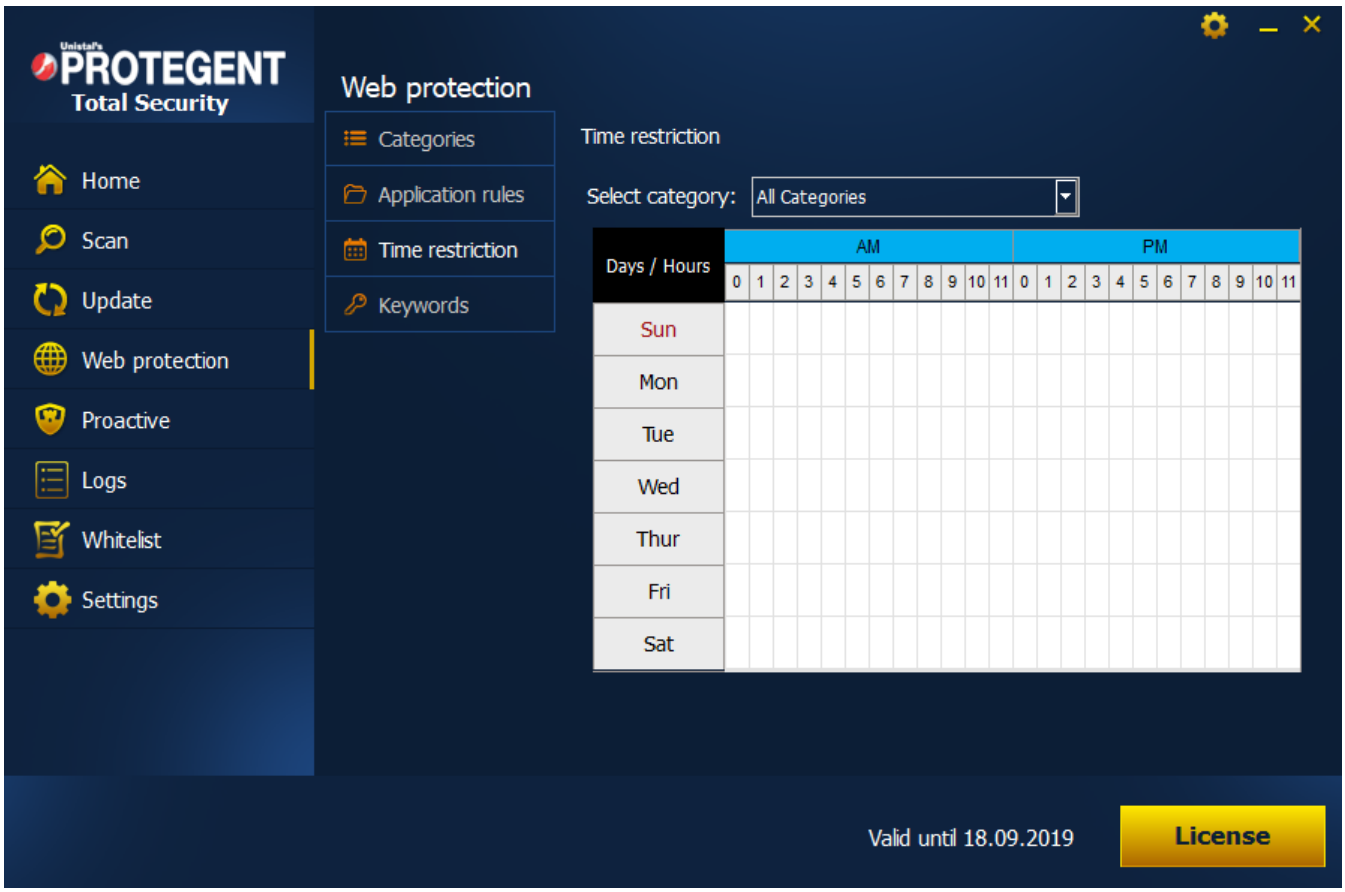


Categories

- This feature ensures Web applications are used exactly as intended in organizations. It protects against the manipulation of Web environment for malicious intentions and provides an added level of security by the application infrastructure. It has a strong defense against known and emerging hacking attacks and has optimal predefined security rules for instant protection.
- With predefined categories you can manage the website blocking.

Time Restriction Feature

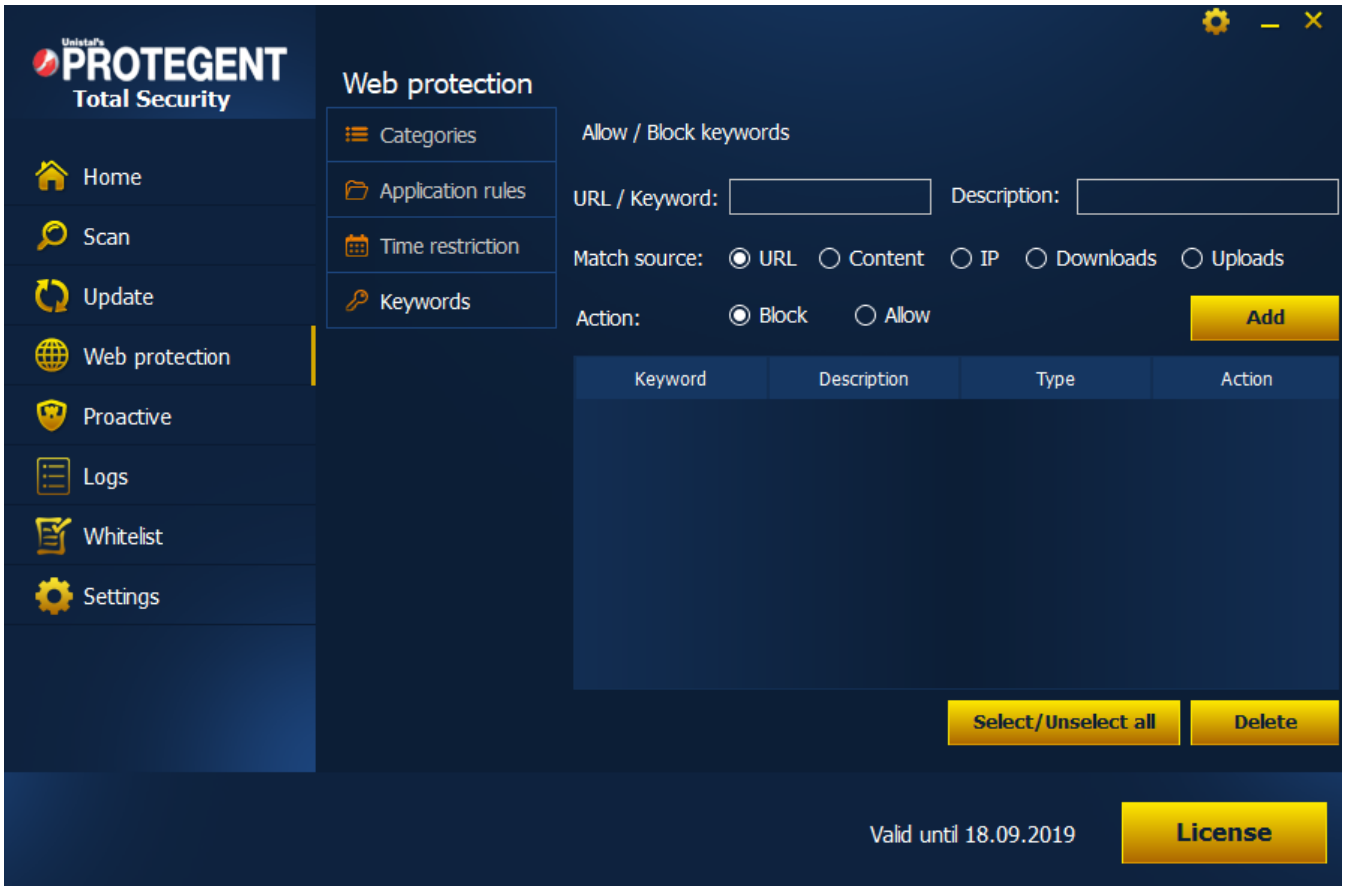
- Protegent® Time Restriction can restrict web access according to a daily time schedule as customize.
- Click “Time Restrictions” in the left-hand column.
- Select category type as all categories or customize as applicable and highlight a block of time during which you wish to deny web access. Once you have selected the time (click and drag the mouse), a menu will pop up to block or allow that time.
- Press the “Save” button.
- Repeat until the Time Restrictions fit your needs.
- You can also allow a Time Selection instead of denying it. Note it is a good idea to save changes as you go.



Keyword Blocking

Enter a keyword, URL or domain name in the Keyword/URL box, fill in the description box and select the match on options under scan type and action, then click “Add”.

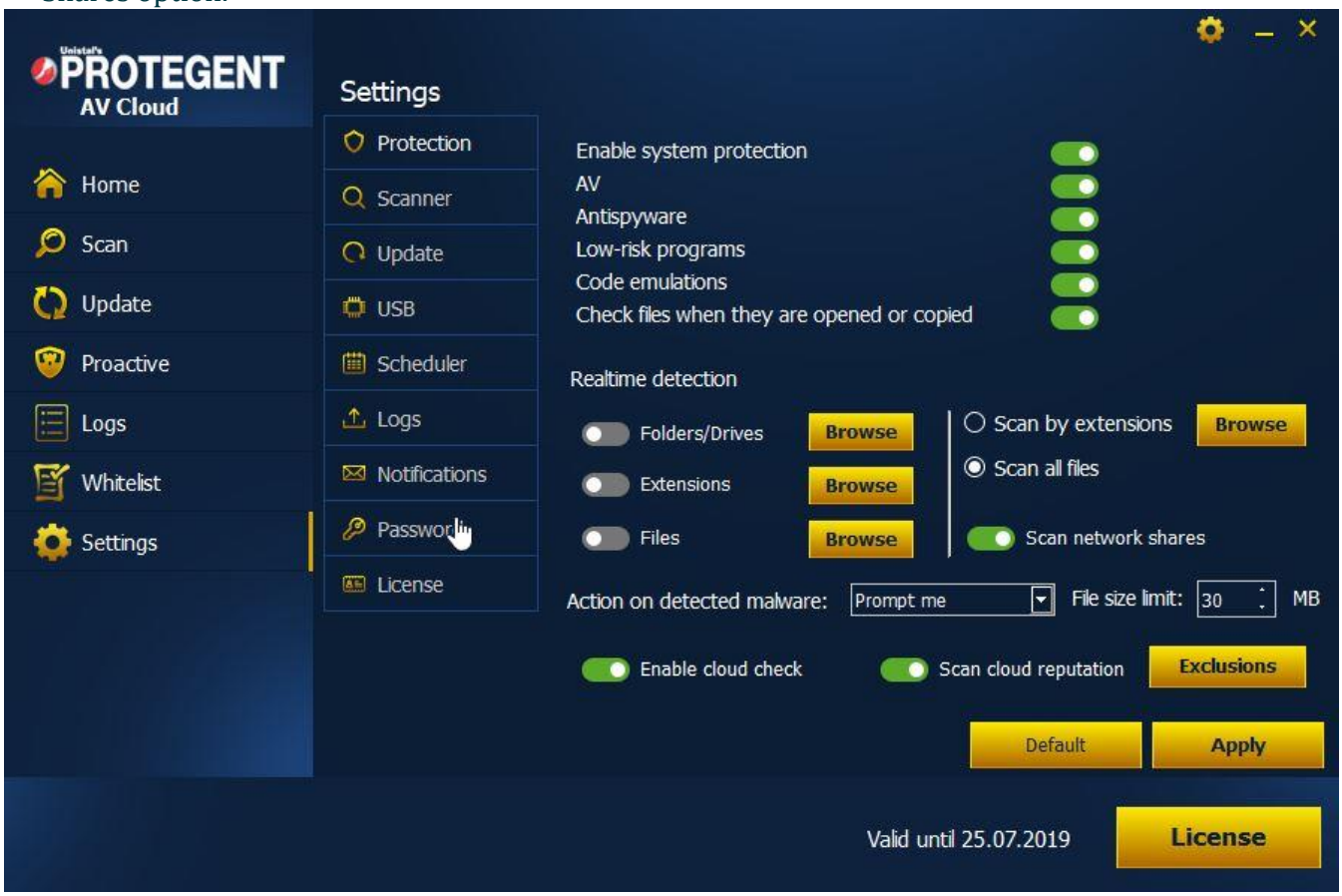
- Some examples of keyword application are: If the keyword “Dating” is specified, the URL <http://www.xxx.com/dating.html> is blocked. If the keyword “.com” is specified,
- Only websites with other domain suffixes (such as .edu or .gov) can be viewed.
- To delete a keyword or domain, select it from the list and click “Delete Keyword”.



SETTINGS

Protection

In the “Protection” tab you are able to enable or disable the scanning options for the devices. The user can also scan particular file extensions present in the system. In real-time detection, user can exclude specific files/folders, extensions and drives from real time protection. Action on detected malware can be select amongst **prompt me** or **repair & backup**. User can also scan the files shared over the network by enabling Scan Network Shares option.

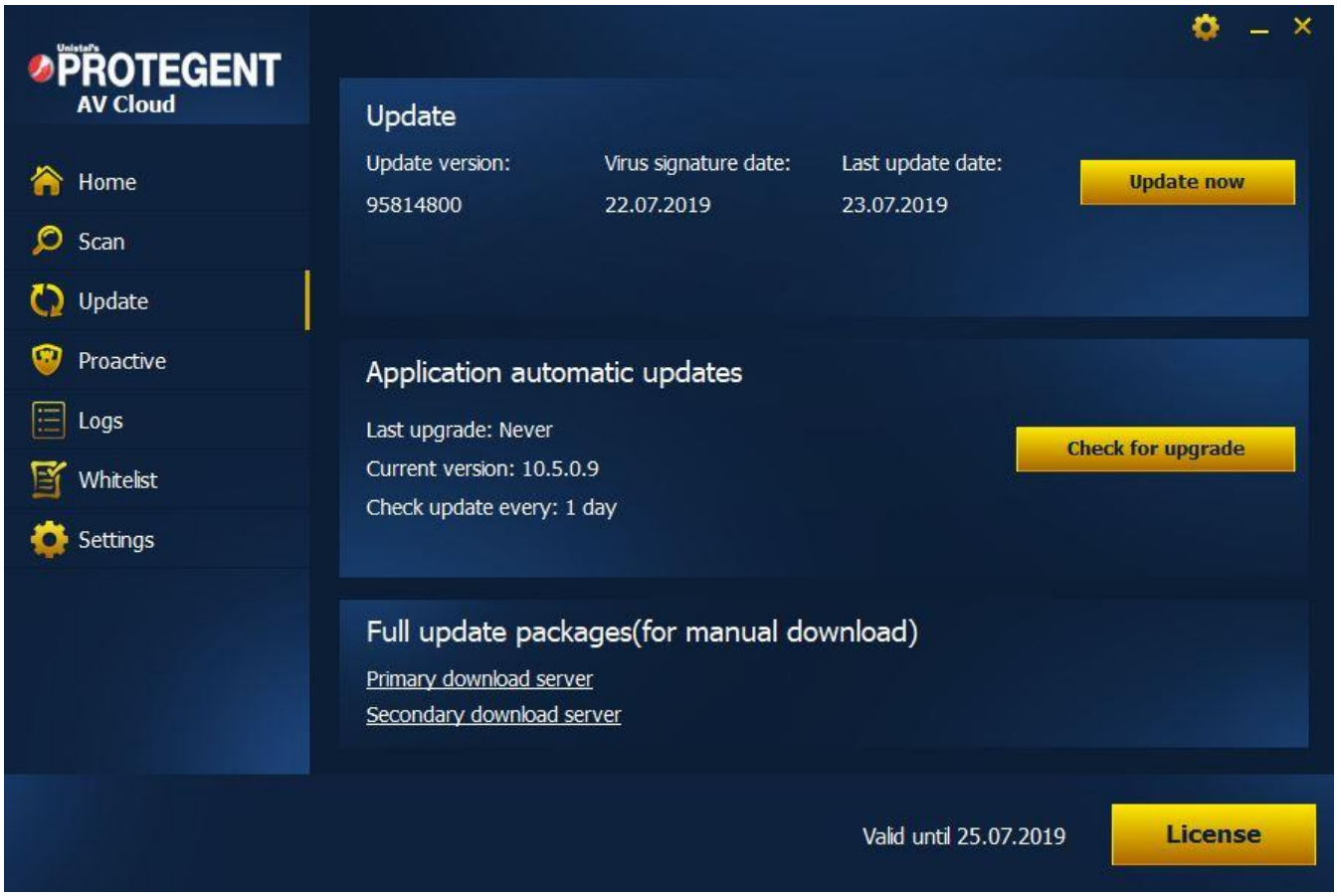


Scanner

In the “Scanner” tab, there are lot more options on scanning. Users can select specific categories which should be scanned from the category list and can also select the scan type (Quick Scan, Full Scan and Custom Scan). User can exclude specific files/folders, extensions and drives from scanning. USB drive insertion behavior can also be selected by user depending on the wish (recommend: perform scan automatically). Recover hidden USB files option allows software to recover any hidden files present in USB.

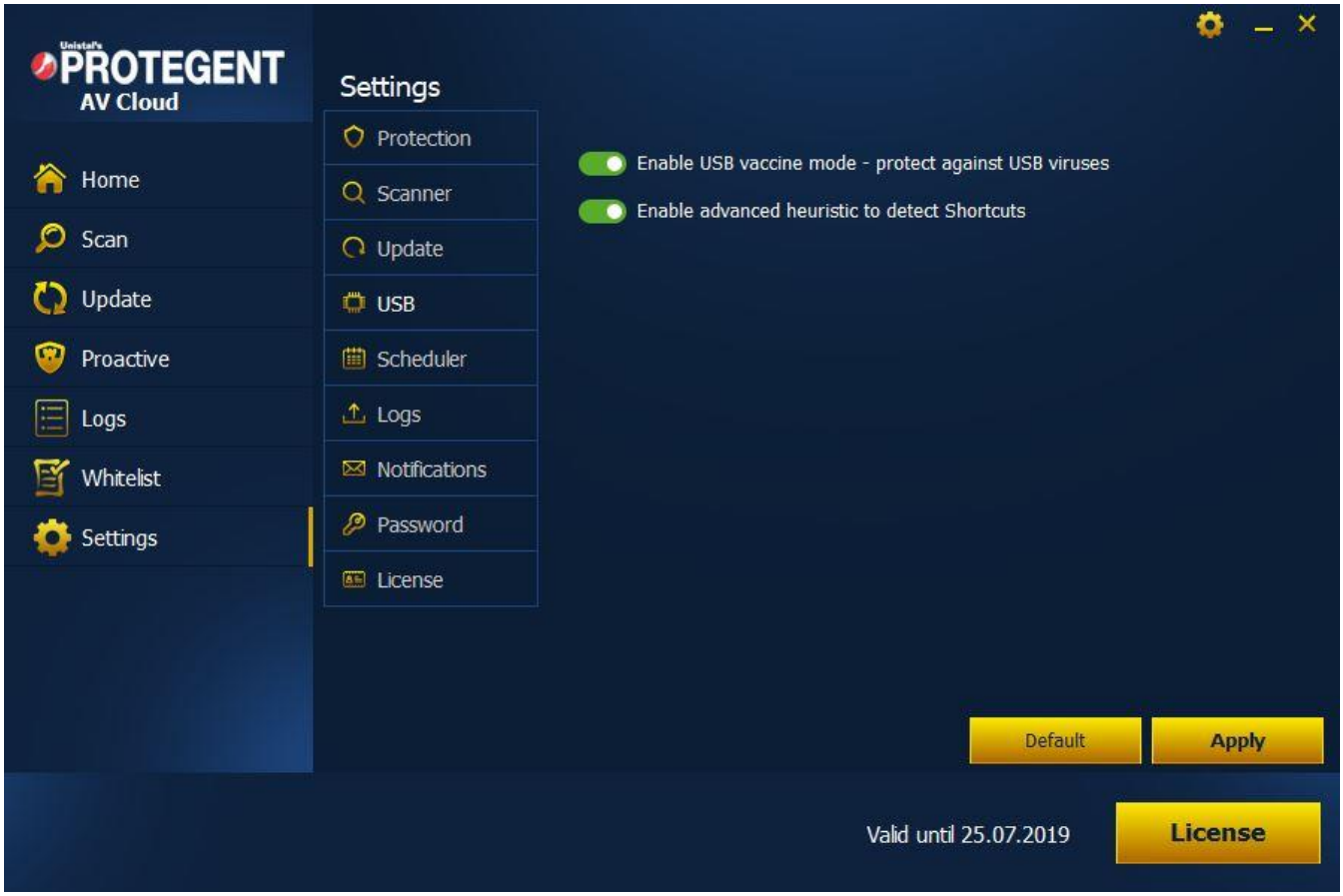
Update

In the Update settings, automatic updates can be enabled and disabled. User can select automatic updates interval in hours. User can also provide proxy server setting to enable the updates to get downloaded from proxy. We have two servers from which the user can select the one from which the updates are downloaded and product is upgraded.



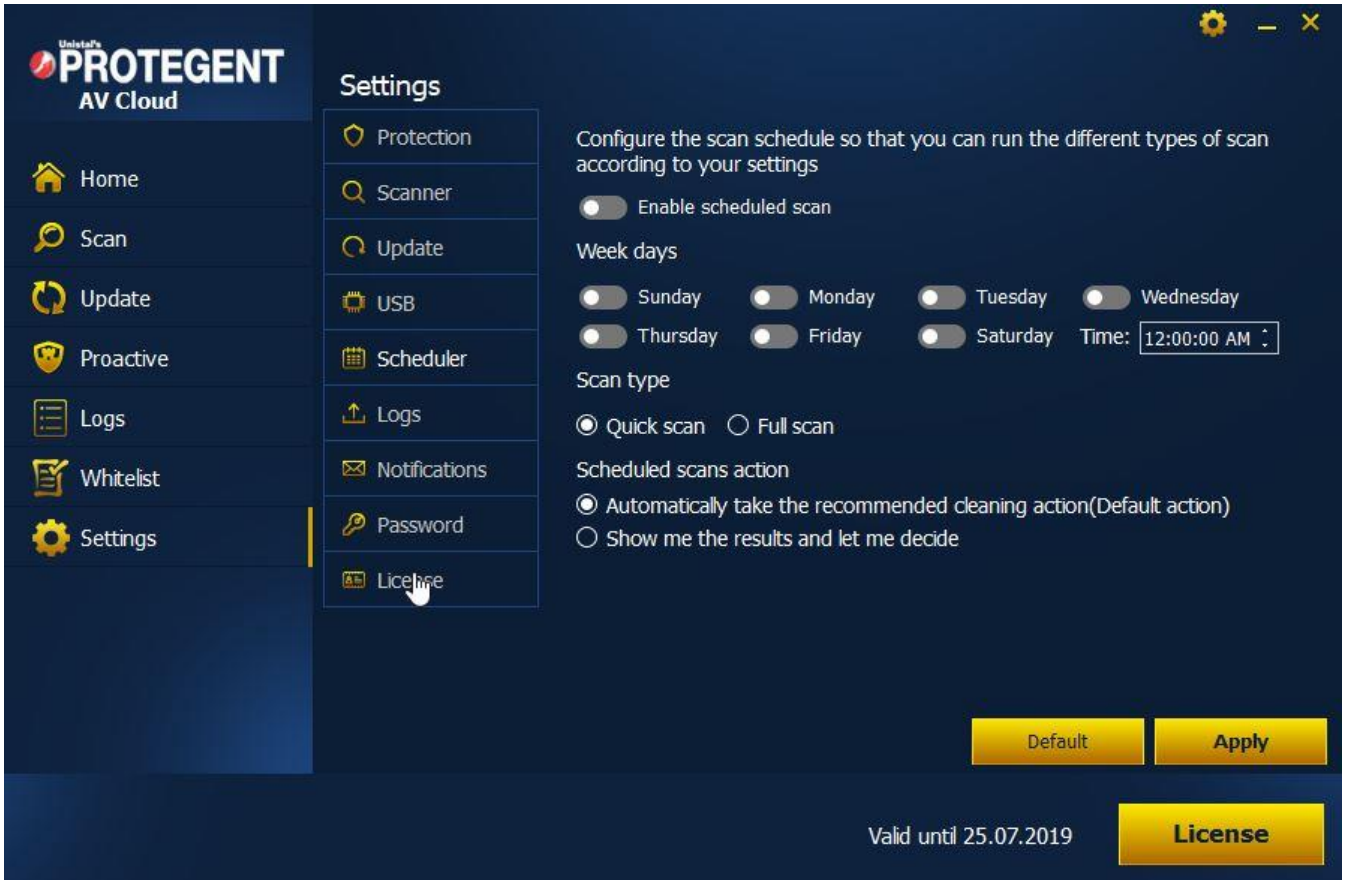
USB

In the USB Tab, user can enable or disable protection against USB viruses. There is an advanced option for enabling advanced heuristic to detect shortcut viruses and even detects the viruses for which the virus definition is not updated in the software.



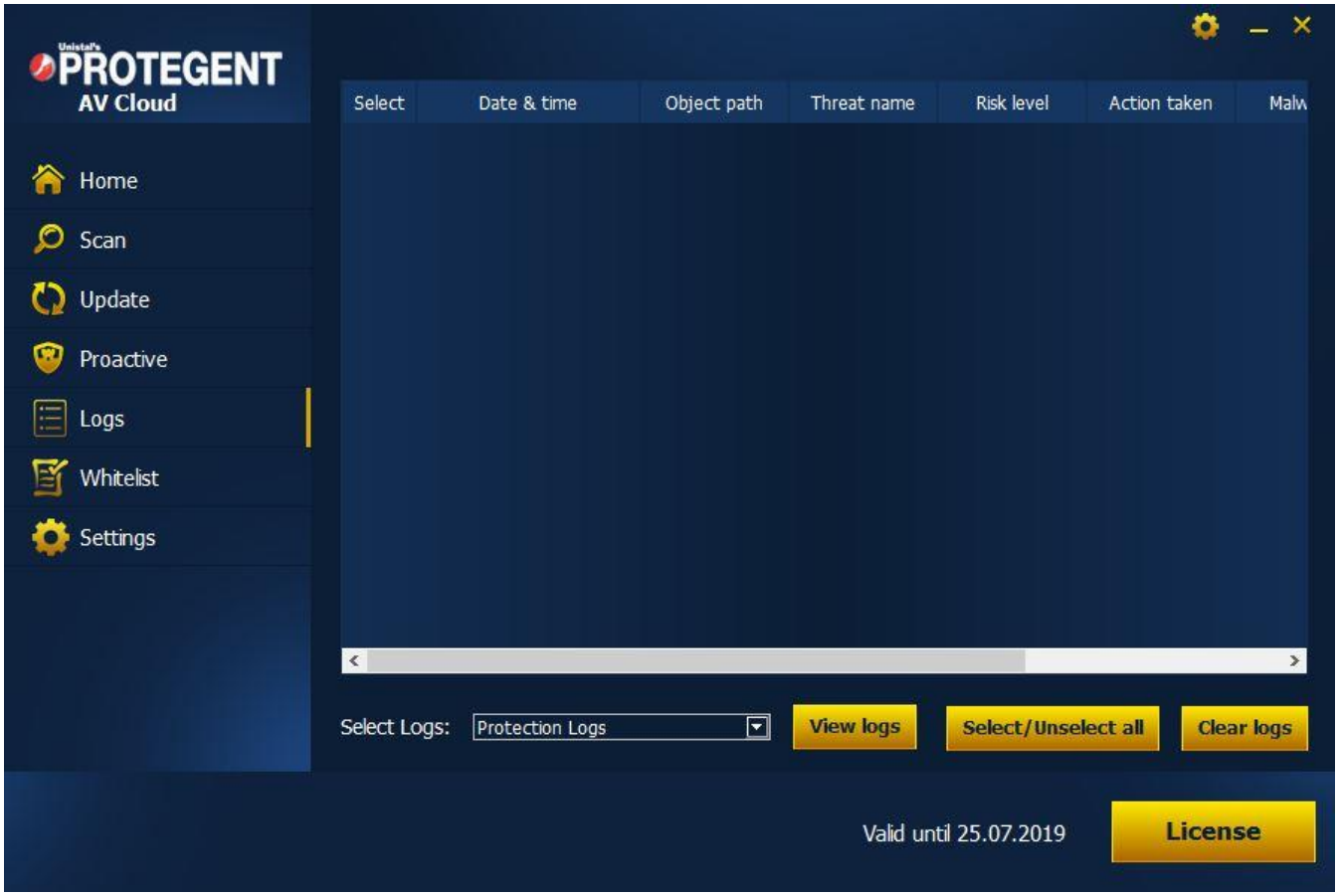
Scheduler

In the Scheduler Tab, user can schedule the scan by enabling it as per choice. User can select the week days, scan type and scheduled scans action.



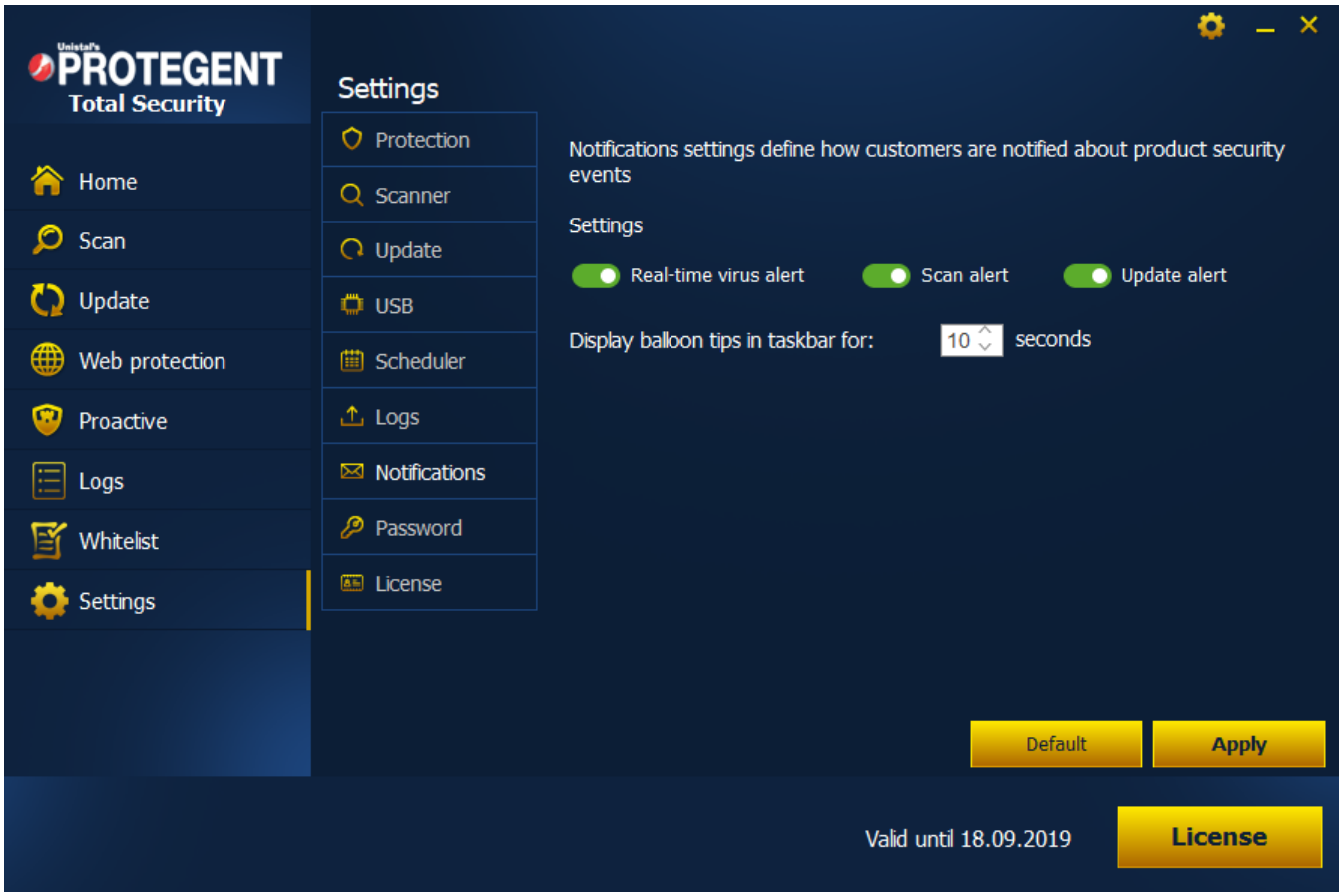
Logs

In the Log maintenance setting, user can define the number of days the logs should be stored on the system before deleting older logs. User can also define the number of days the quarantine logs should be maintained before deleting older logs.



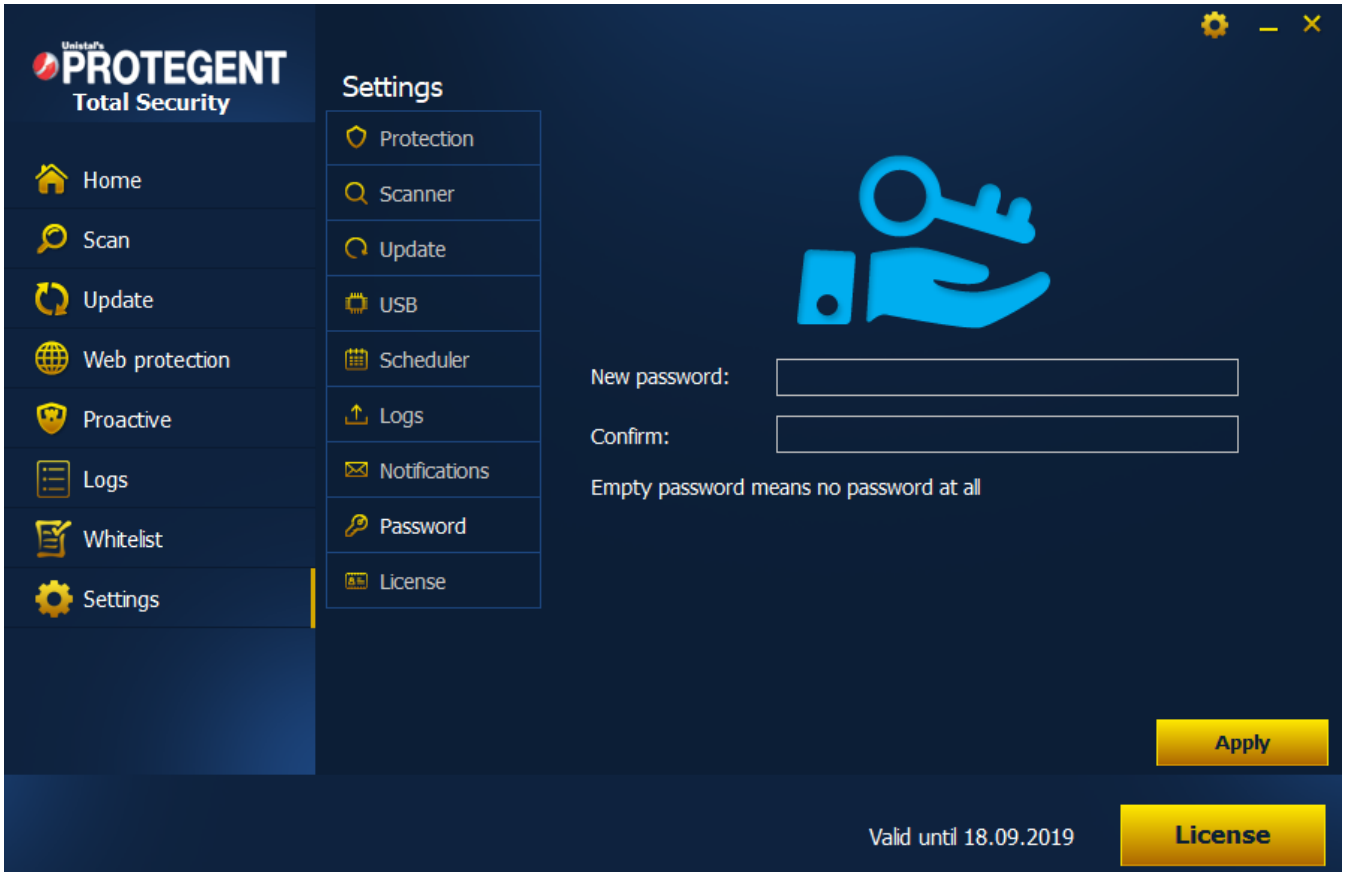
Notifications

Notification settings tab allows the user to define how they get notified about the product security events. User can also set the duration of the notification which is displayed as balloon tips in taskbar.



Password

In the password setting tab, user can provide a password to the software so that unauthorized users can't changes the setting done by the admin.

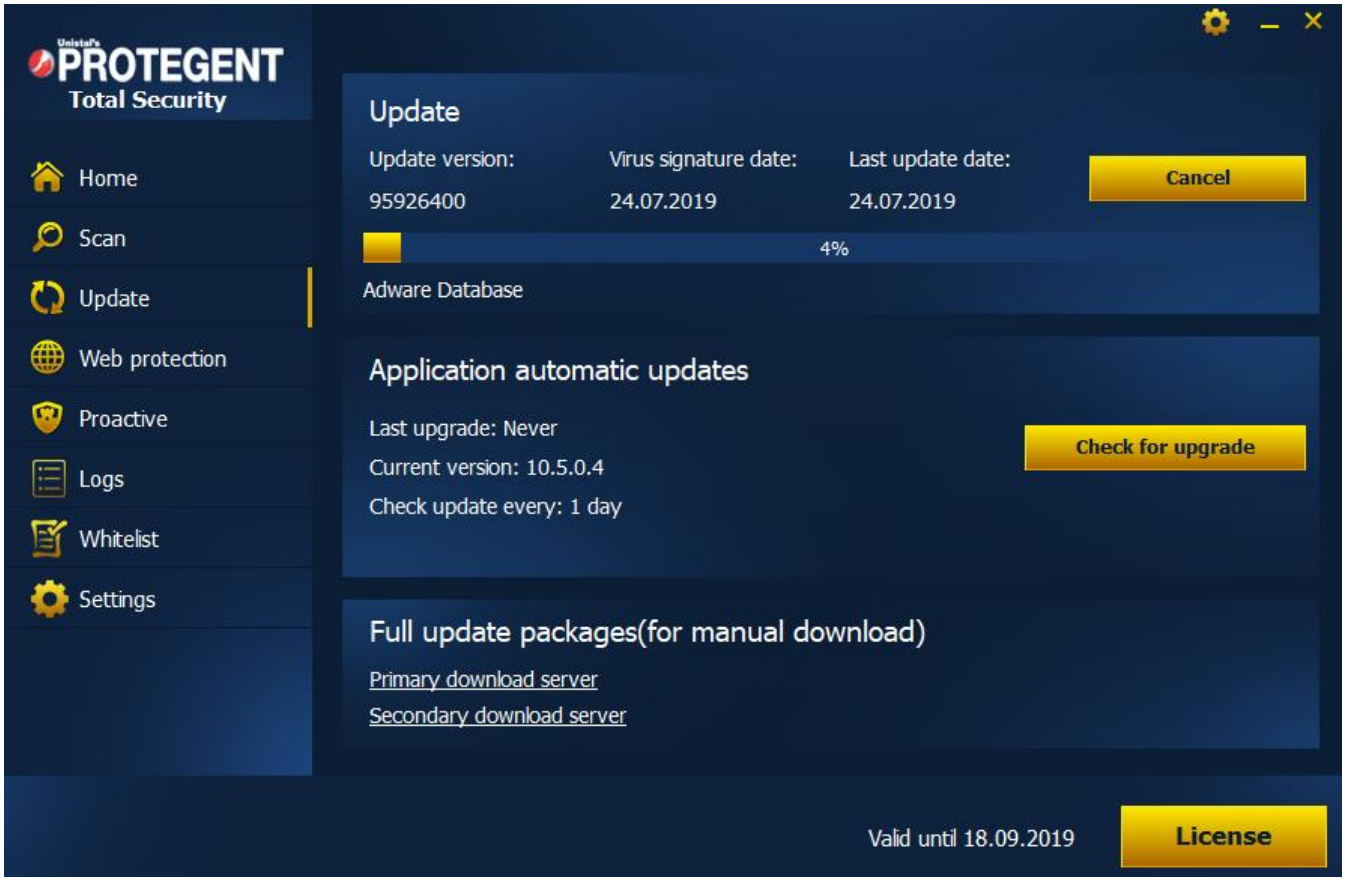


License

In the license tab, user gets the product activation details which include the validity of the product and the license type. From here, user can register the product using the credential provided during the purchase. There is an option to buy the product directly by clicking the Buy Now! Button.

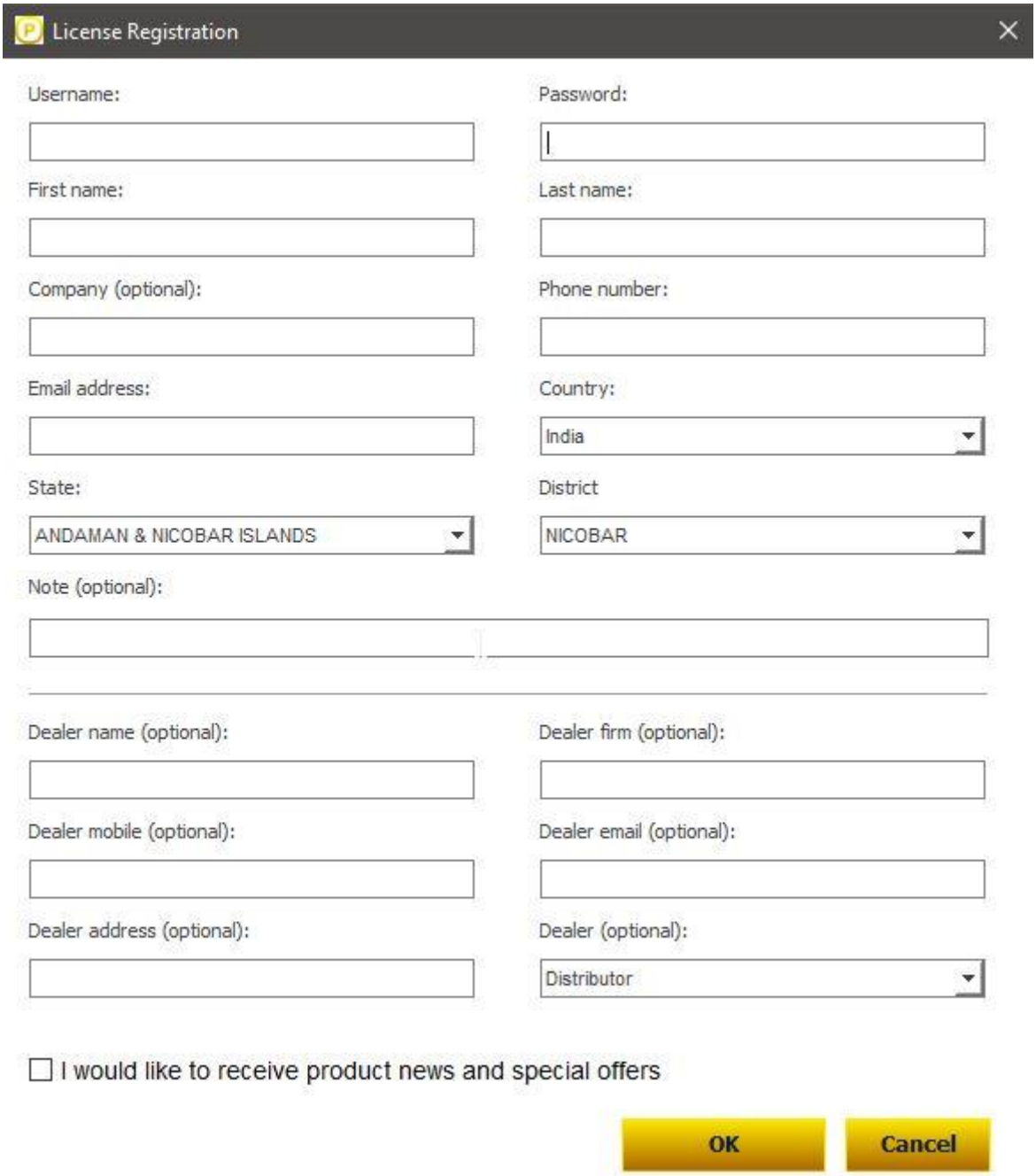
UPDATE

User can update the software by clicking over the **Update Now** button. User can also download the latest version of the software by clicking on **Check for Upgrade**. For offline update user can download it manually from either primary or secondary download server.



LICENSE

User can register the license by filling out the necessary details along with the username and password received during the purchase.

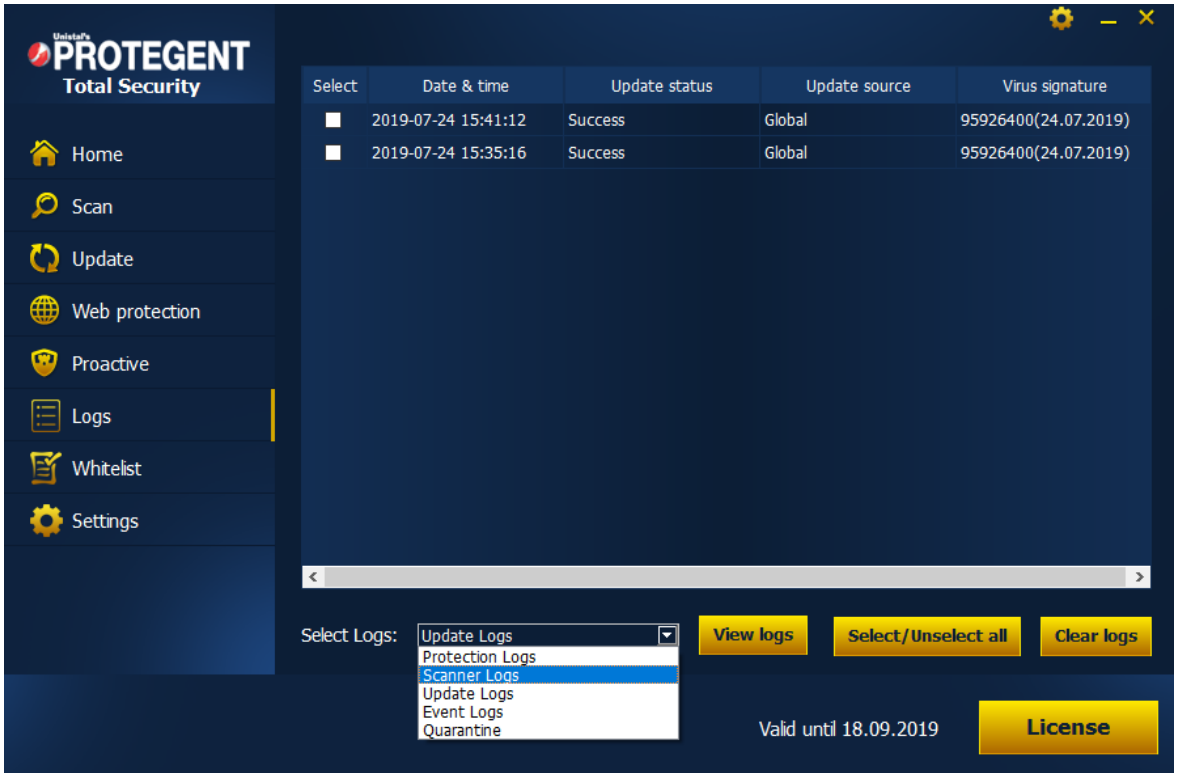


ABOUT

After clicking over the about button, a pop-up windows will appear as below which contains information about the software product. It contains information related to definitions version, last definition update date, version of the software product, email contact of sales & support team. It also includes the Toll Free which users can use for any queries.

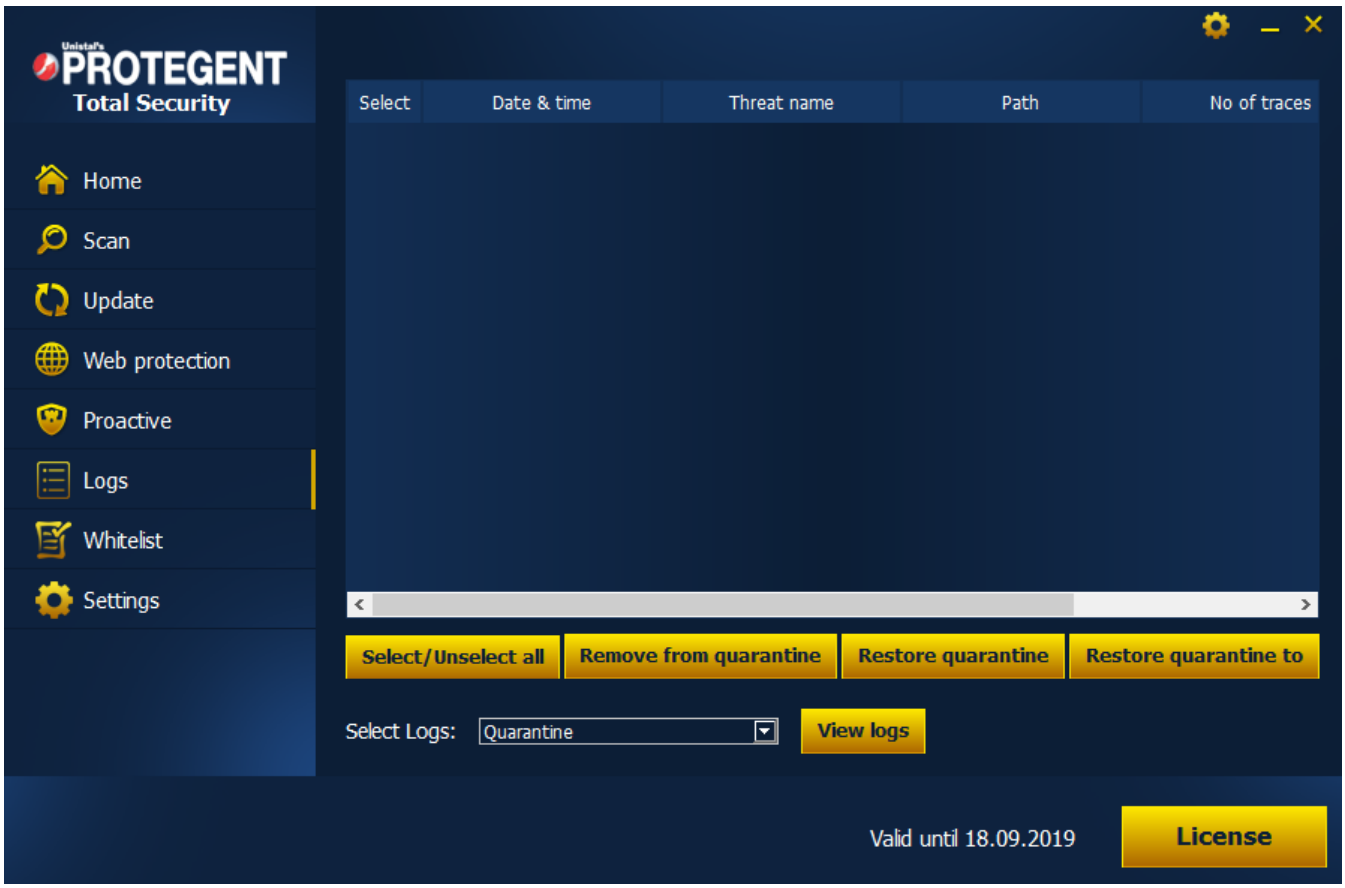
LOGS

In the Menu, select the logs option which will open a pop-up window as displayed below. User can view the logs of various categories like protection, scanner, update, event and quarantine



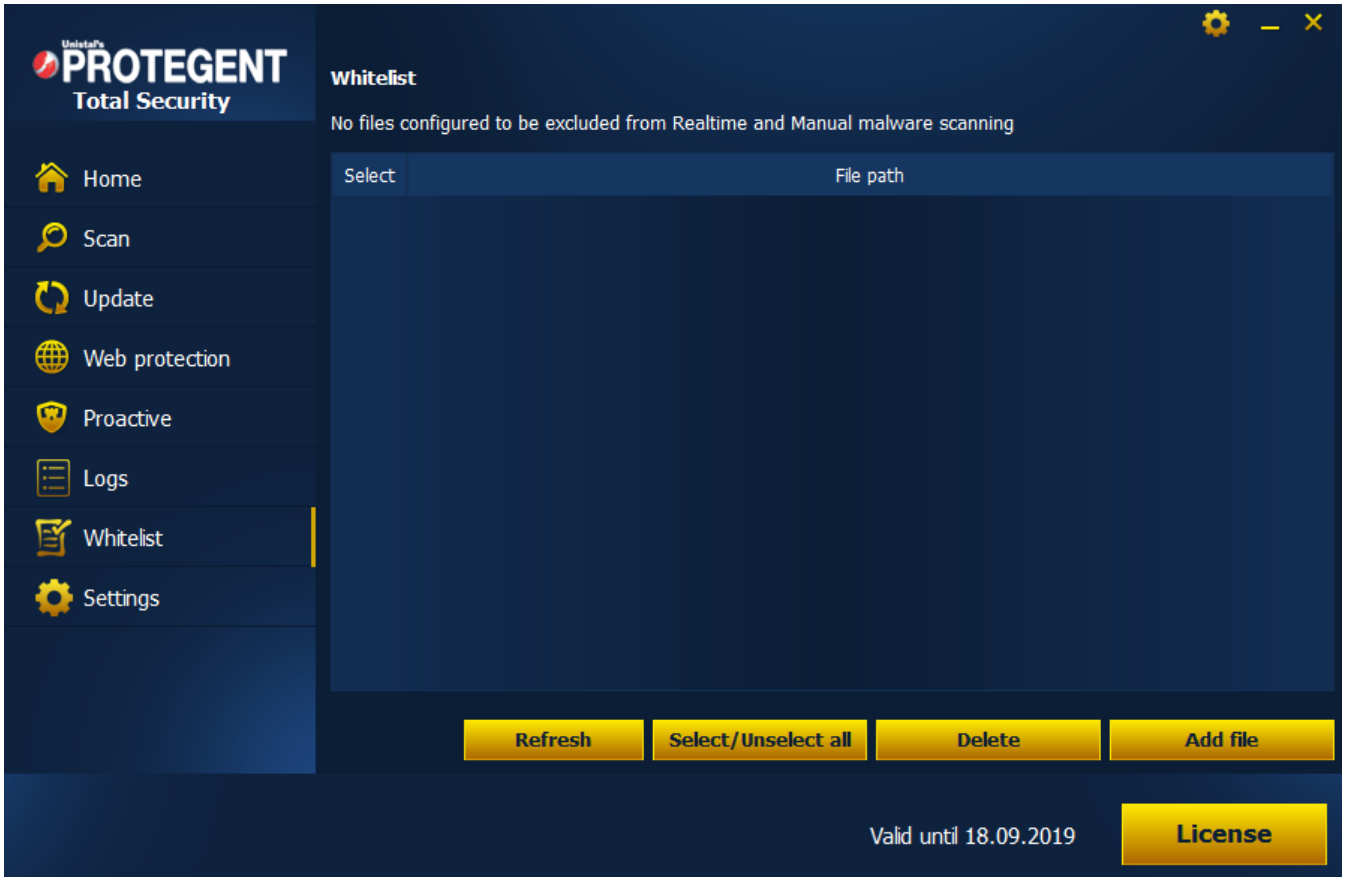
QUARANTINE

User can see the infected files and unknown viruses which has been detected by software and kept in the quarantine. From here, user can clear the quarantine to permanently delete the files present in it. User can also restore the files present in the quarantine to a specific location.



WHITELIST

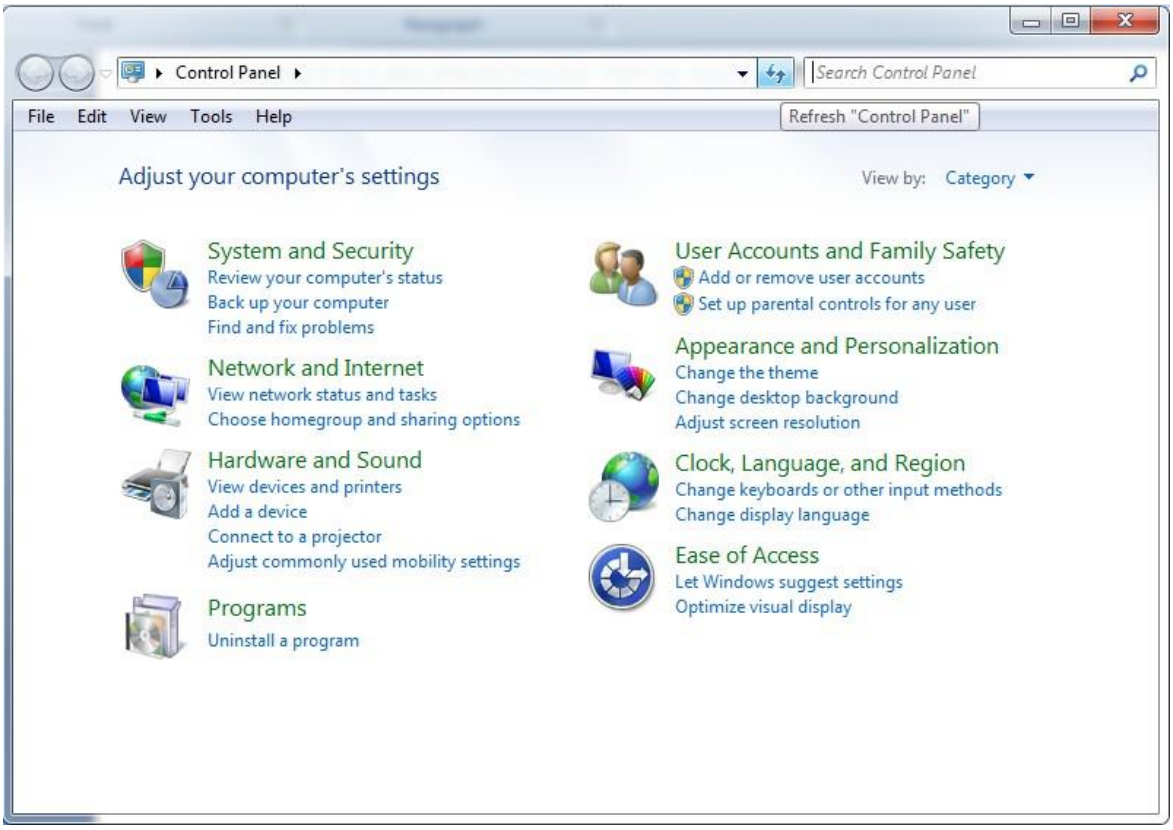
User can manually select specific files from the system which are excluded from real-time and manual scanning.



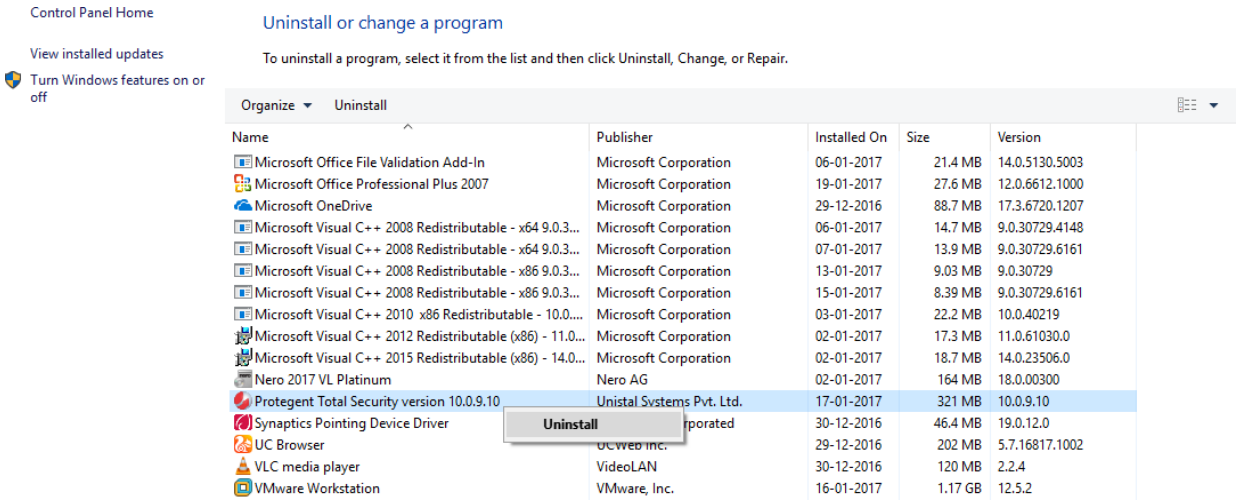
UNINSTALLING PROTEGENT TOTAL SECURITY

To uninstall the Protegent Total Security, click on the “Start Menu” button on the taskbar then go to “Control Panel”.

- In control Panel screen, click on **Uninstall a program** option

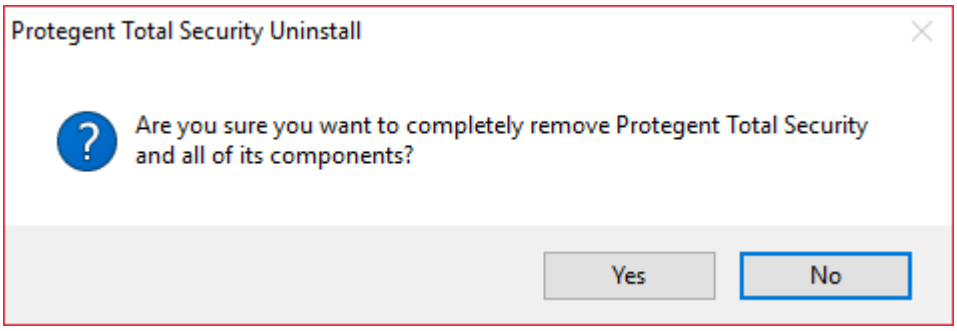


- This will navigate you to a list of the system programs that you have installed. Select “Protegent Total Security Version” program and right click. It will then show you the option to uninstall the program as shown in the image.

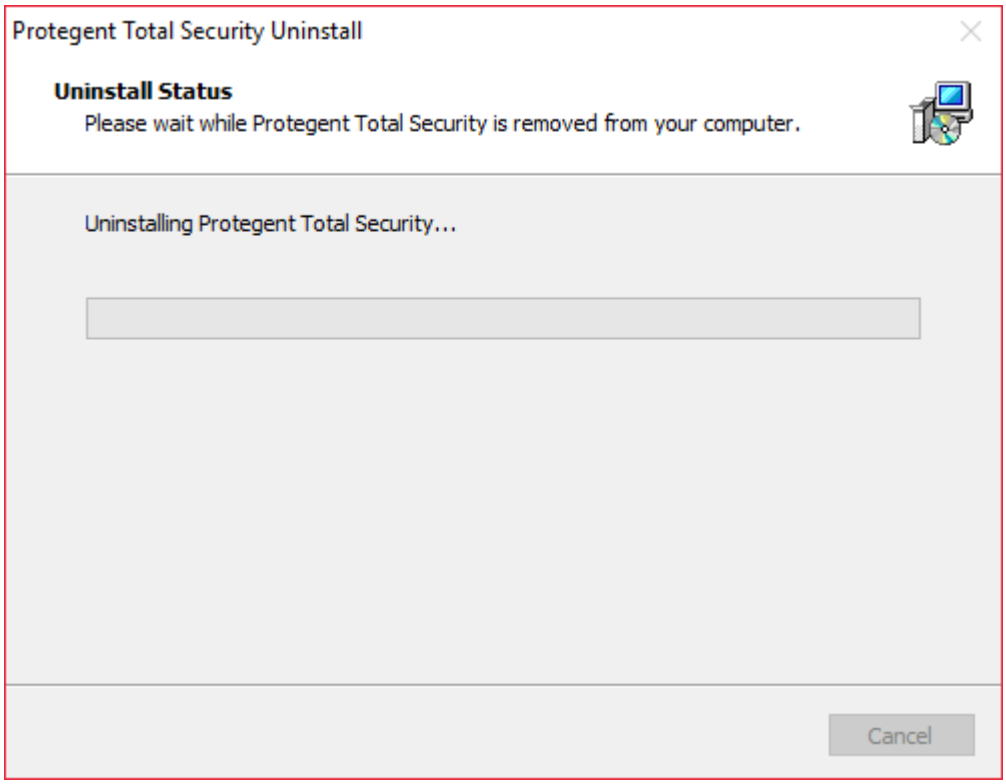


- Click on “Un-install” and follow the process to un-install.

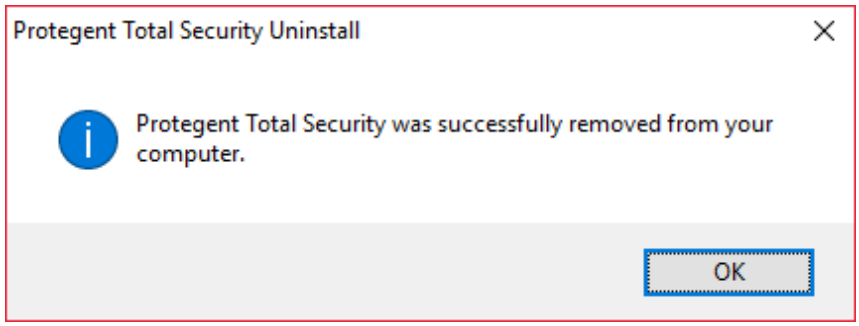
- One dialogue box will appear where it will ask for the last time “Are you sure you want to completely remove Protegent Total Security and all of its components”



- Then the process of un-installation will start and continue until the whole green colored bar is filled.



- It will display the successfully uninstalled message as below.



Technical Support:

For Technical Support on Protegent® Products, please visit http://protegent360.com/

Sales: isales@unistal.com
Support: support@unistal.com
Website:
http://protegent360.com/