

# Protegent<sup>®</sup>

## 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](http://www.protegent360.com)

Protegent<sup>®</sup> 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.

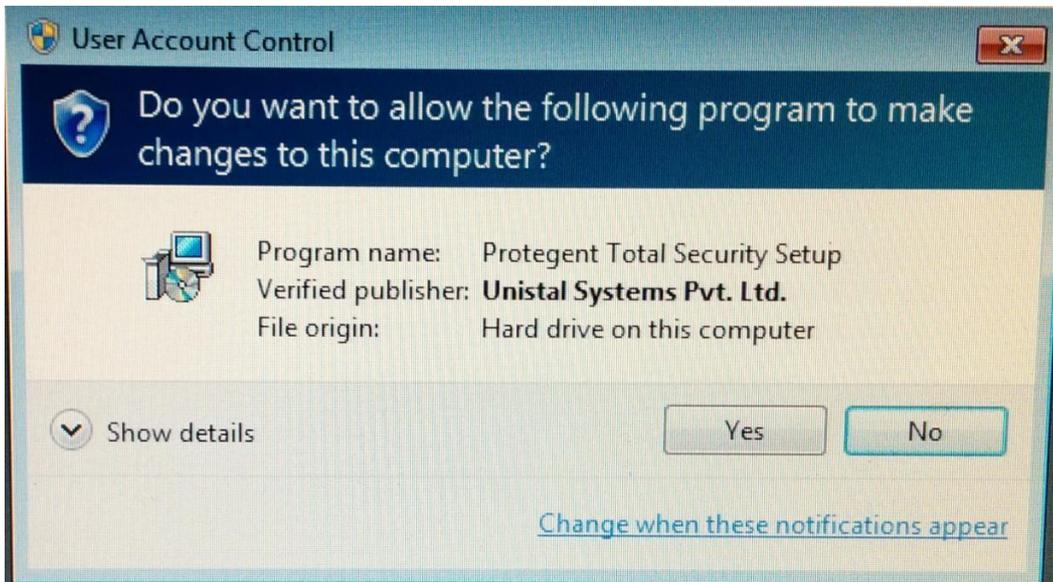
**Install:** The installation program runs in a self-explanatory dialog mode. Every window contains a certain selection of buttons to control the installation process.

### **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:



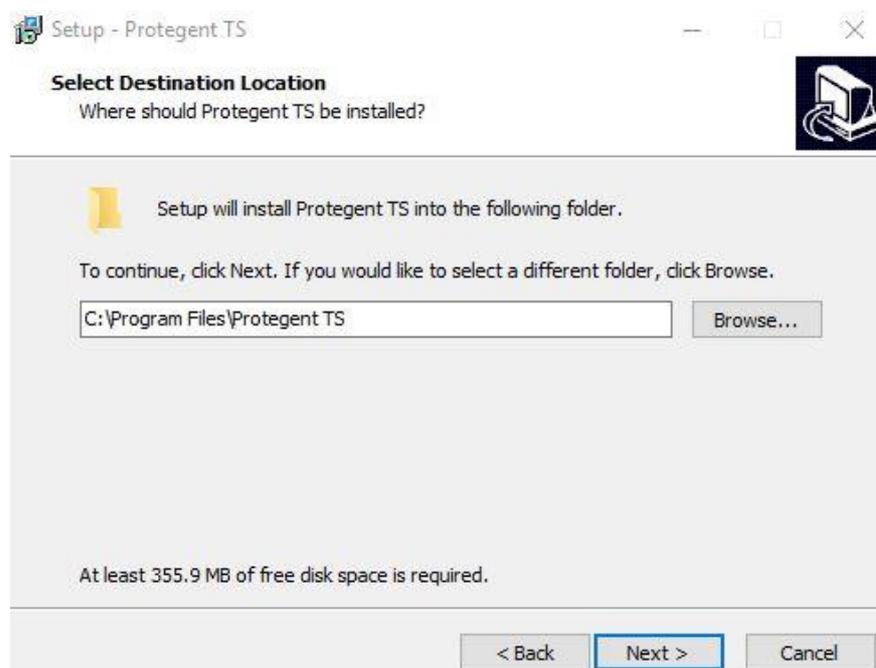
- Click “Next” and the installation Wizard will then guide you through the rest of the installation process.



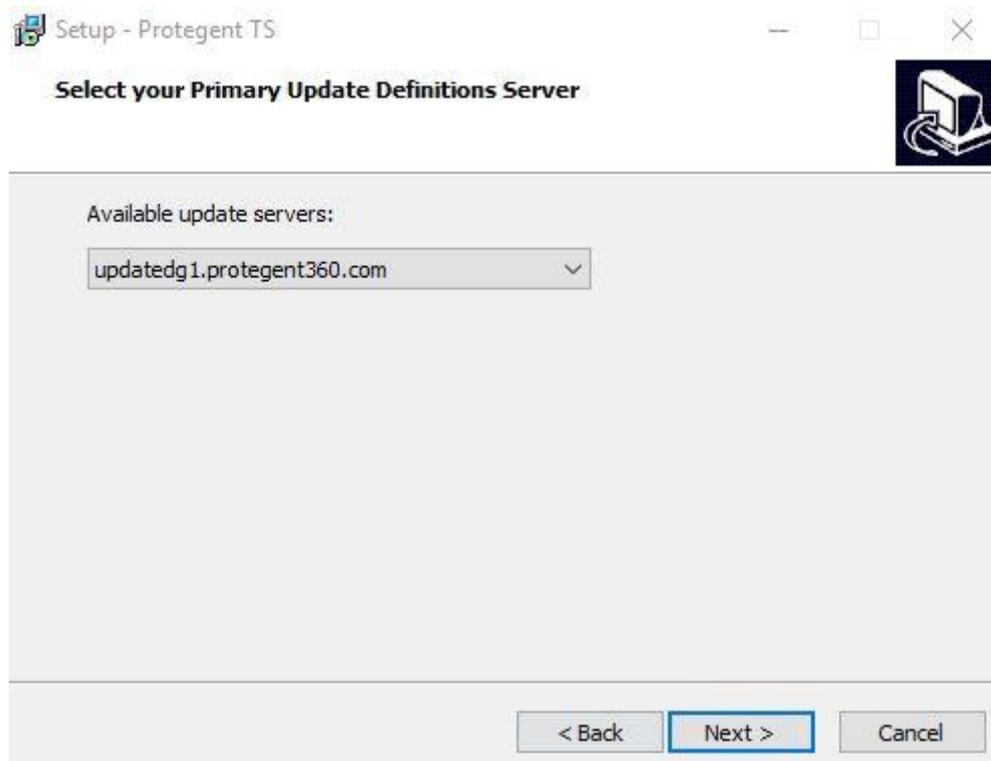
- First you will be asked to read about the minimum system requirements and then confirm that you to agree to the end-user license conditions.



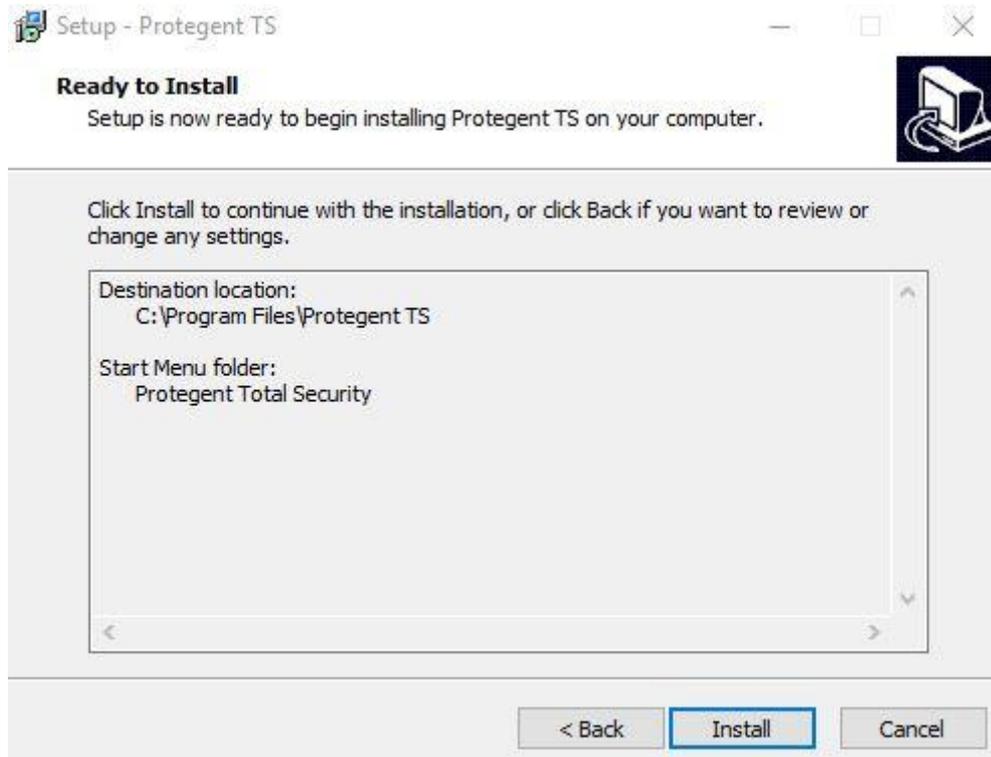
- To continue, click on “I accept the agreement”, this enables “Next” for further steps.
- Clicking on “Next” will navigate you to the destination selection window.
- You will be asked to confirm the destination directory, i.e. where the program files will be saved. The program will select this automatically 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.



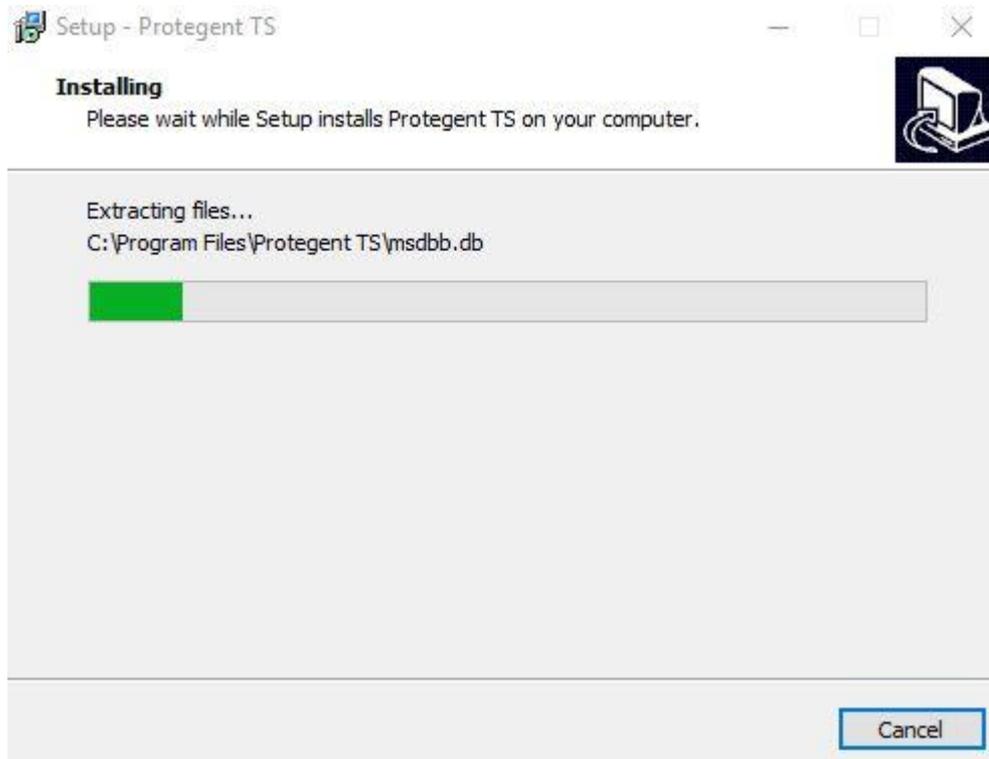
- The user selects your “updatedg1.protegent360.com” as Primary Update Definitions Server.



- 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.

**License Registration**

Username:

Password:

First name:

Last name:

Company (optional):

Phone number:

Email address:

Country:

State:

District:

Note (optional):

---

Dealer name (optional):

Dealer firm (optional):

Dealer mobile (optional):

Dealer email (optional):

Dealer address (optional):

Dealer (optional):

I would like to receive product news and special offers

**OK** **Cancel**

- 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.

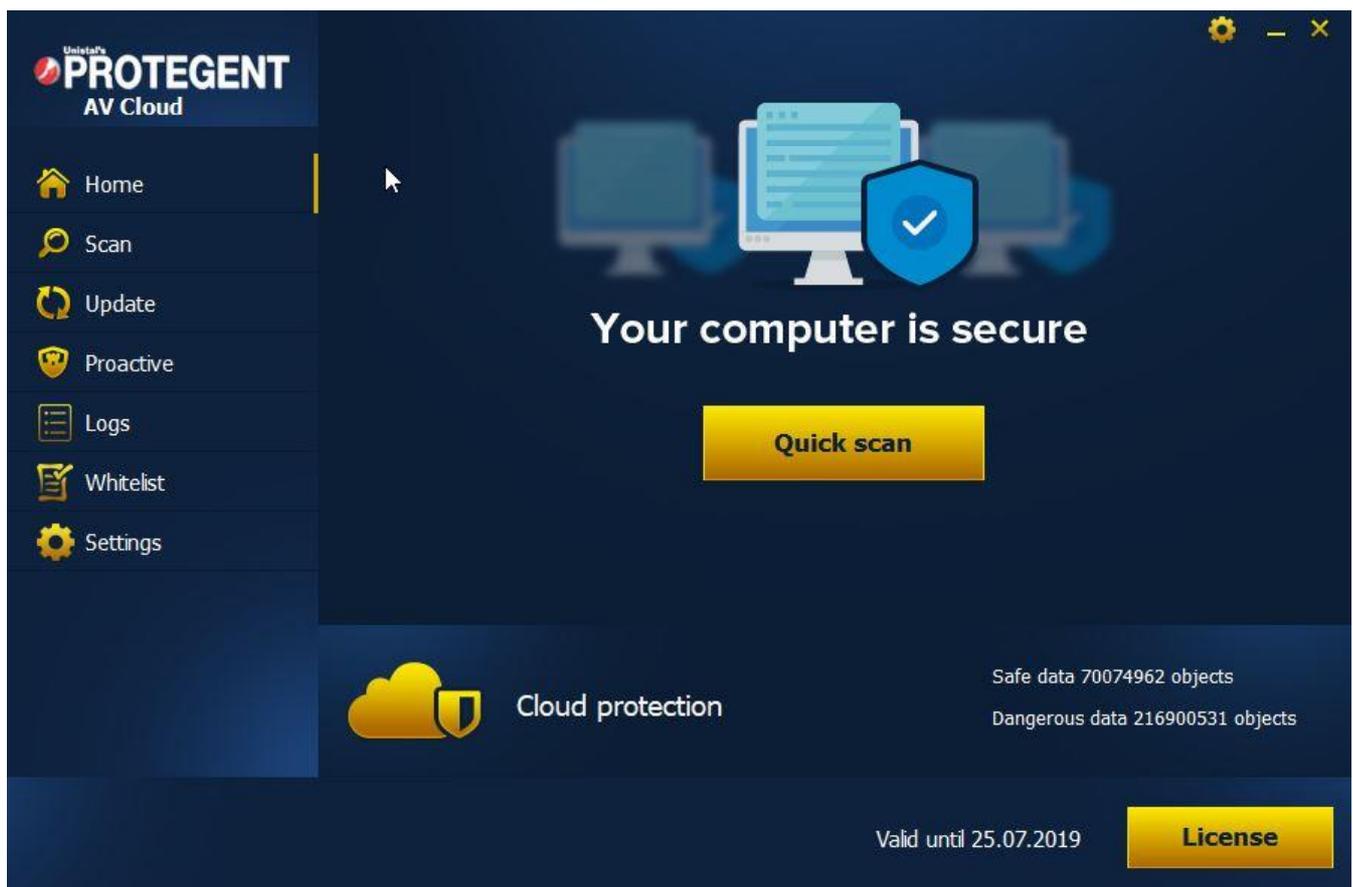
## WORKING WITH PROTEGENT TOTAL SECURITY

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.

**Unistal's PROTEGENT Total Security**

- Home
- Scan
- Update
- Web protection
- Proactive
- Logs
- Whitelist
- Settings

**Total security**

Total Security is able to safeguard your computer while you are online. Each time you are visiting harmful or suspicious site you'll be notified about this issue.

**Web filtering statistics**

Index	Value
1	5
2	3
3	2
4	3
5	2
6	1
7	2
8	5
9	3
10	10

**On-run protection**

Advanced protection against suspicious system activity. It immediately detects malware before it harms your PC.

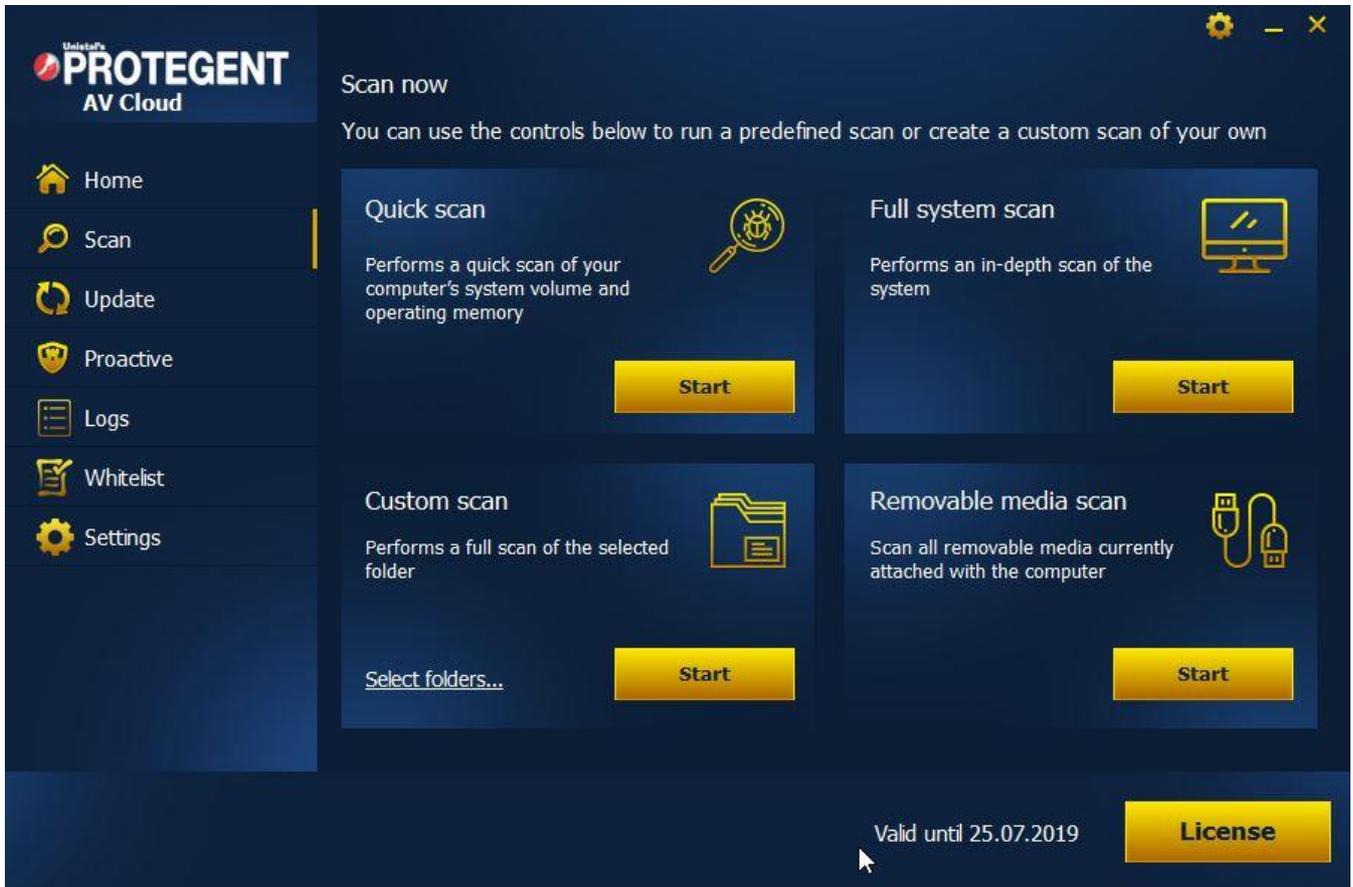
**Removable device**

Scan all your removable disks plugged into your computer (flash drives, memory sticks). If any threats detected you'll be notified at once.

Valid until 18.09.2019 [License](#)

## SCAN

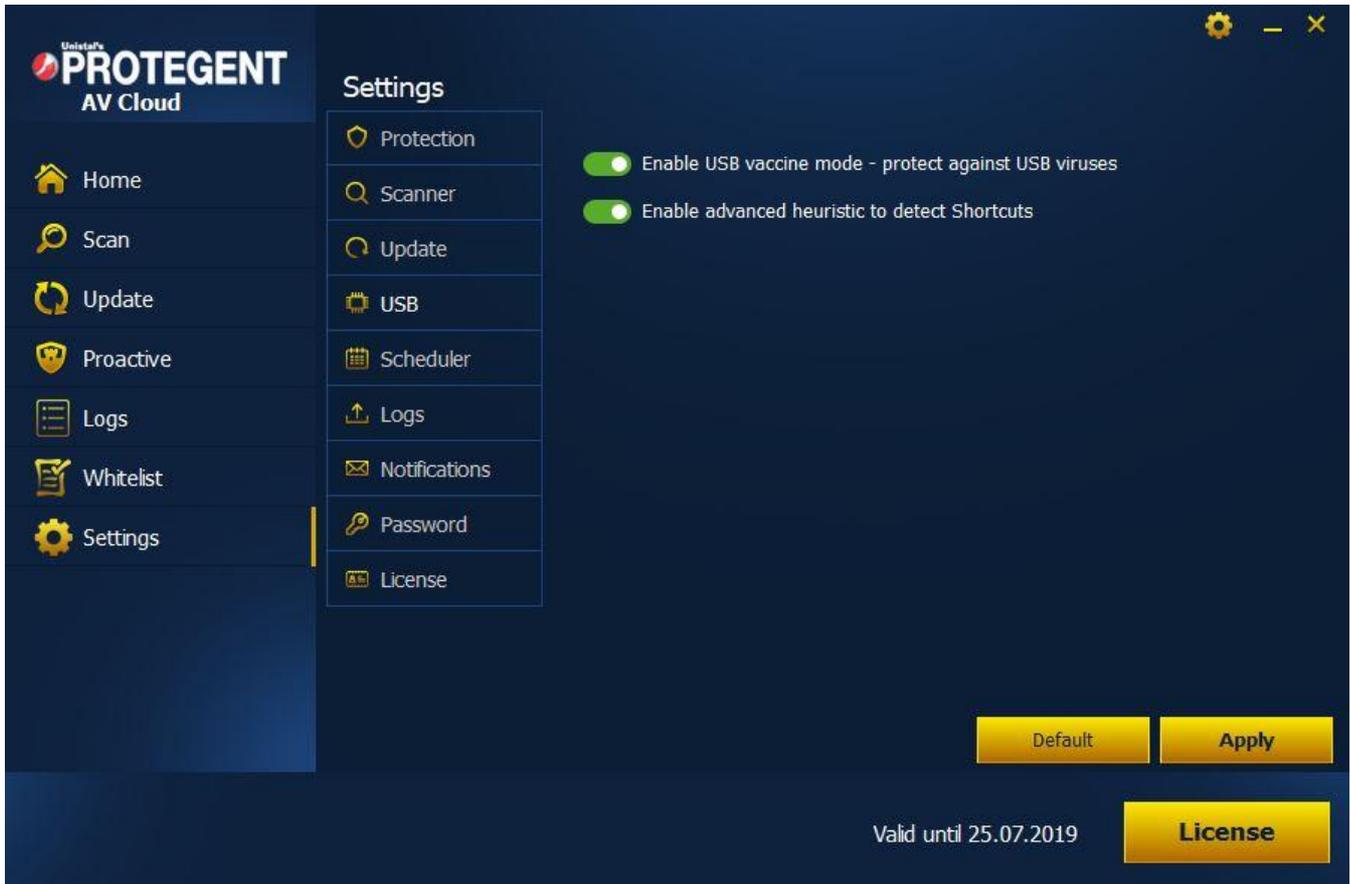
- If you want to run quick, full system scan, external devices or specific folders scan in your system then select the respective “Scan” option.



- 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.

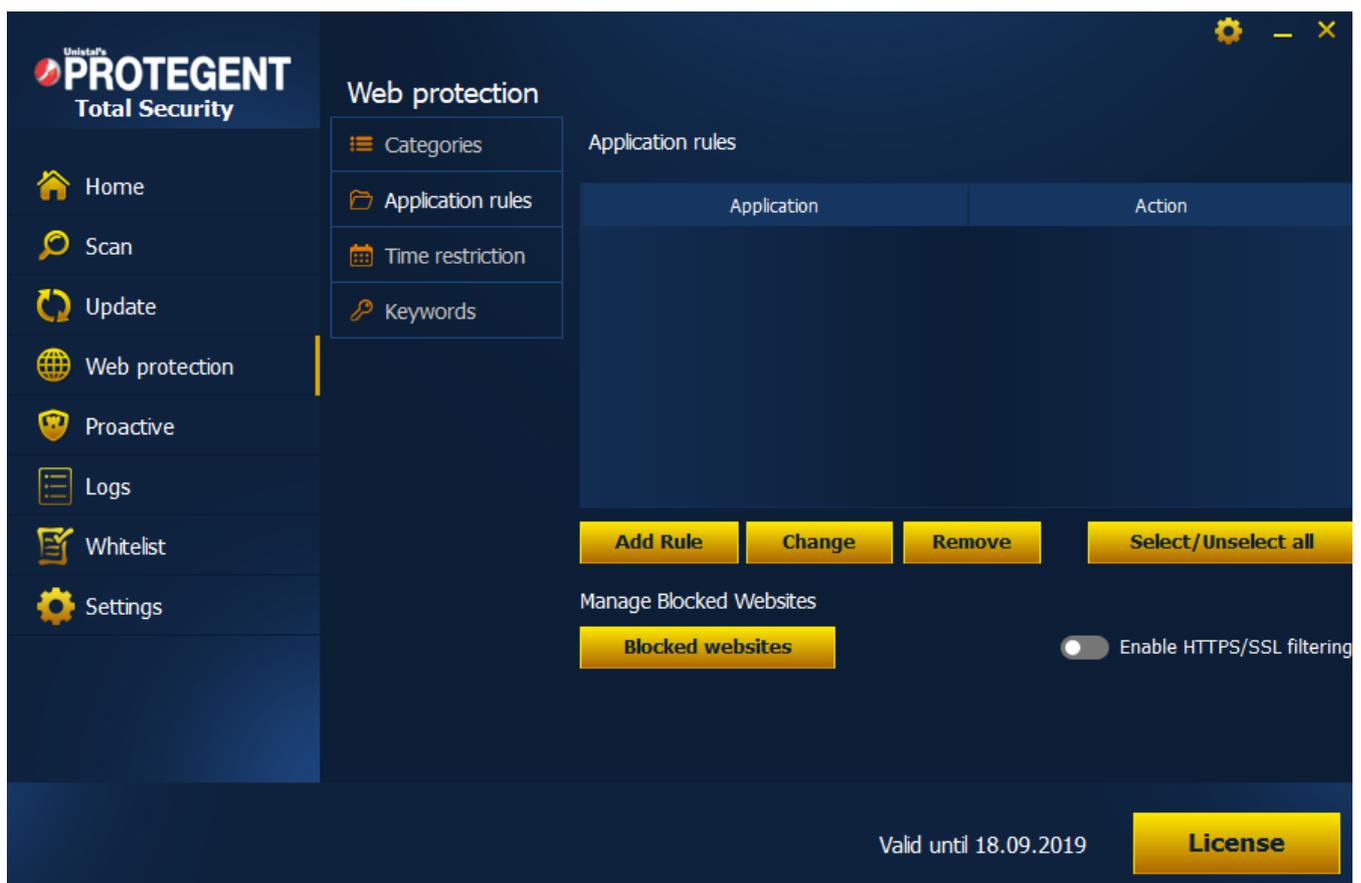
- You can configure the Protegent® category from the application.
- In the application based URL categorization, each row represents one feature. You simply have to check or uncheck checkboxes to enable or disable the features under the Categories section.
- When a check box is checked, then that particular 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.

The screenshot displays the 'Web protection' configuration window in Unistal's Protegent Total Security. The interface is dark-themed with a blue sidebar on the left containing navigation icons for Home, Scan, Update, Web protection (highlighted), Proactive, Logs, Whitelist, and Settings. The main panel is divided into several sections: 'Web protection' with sub-options for Categories, Application rules, Time restriction, and Keywords; 'Web filtering statistics' showing a bar chart with a peak of 10; 'Enable All' and 'Disable All' buttons; a list of 'Unethical' categories with toggle switches for Aggressive, Malware, Phishing, DDos, Virus infected, Hacking, Spyware, Violence, and Dialers; and a list of 'Adult and controversial' categories including Computers & Internet, Business interests, Personal interests, and Unrated. At the bottom right, it shows 'Valid until 18.09.2019' and a yellow 'License' button.

## Application Rules

Protegent<sup>®</sup> 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.

The screenshot displays the 'Web protection' settings in Unistal's PROTEGENT Total Security. The interface is dark-themed with yellow accents. On the left is a sidebar with navigation icons for Home, Scan, Update, Web protection (selected), Proactive, Logs, Whitelist, and Settings. The main content area is divided into several sections:

- Web protection:** A sub-menu with options for Categories, Application rules, Time restriction, and Keywords.
- Web filtering statistics:** A bar chart showing filtering levels for different categories. The y-axis ranges from 0 to 10. A prominent yellow bar reaches the 10 mark, while other bars are much shorter.
- Control Buttons:** Two yellow buttons labeled 'Enable All' and 'Disable All'.
- Unethical:** A section with a scrollable list of toggle switches for various threats: Aggressive, Malware, Phishing, DDoS, Virus infected, Hacking, Spyware, Violence, and Dialers. All switches are currently turned off.
- Categories:** A list of predefined categories including Adult and controversial, Computers & Internet, Business interests, Personal interests, and Unrated.

At the bottom right, there is a license information section showing 'Valid until 18.09.2019' and a yellow 'License' button.

### 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.

The screenshot shows the Protegent Total Security web protection interface. On the left is a navigation menu with options: Home, Scan, Update, Web protection (selected), Proactive, Logs, Whitelist, and Settings. The main area is titled 'Web protection' and contains sub-sections: Categories, Application rules, Time restriction (selected), and Keywords. The 'Time restriction' section shows a dropdown menu for 'Select category:' set to 'All Categories'. Below this is a grid for selecting time restrictions. The grid has columns for 'Days / Hours' (Sun-Sat) and 'Hours' (0-11 for AM and 0-11 for PM). The 'Sun' row is highlighted in red. At the bottom right, there is a license information section showing 'Valid until 18.09.2019' and a yellow 'License' button.

Days / Hours	AM											PM												
	0	1	2	3	4	5	6	7	8	9	10	11	0	1	2	3	4	5	6	7	8	9	10	11
Sun																								
Mon																								
Tue																								
Wed																								
Thur																								
Fri																								
Sat																								

## 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”.

The screenshot displays the 'Web protection' settings in the PROTEGENT Total Security application. The interface is dark-themed with yellow accents. On the left is a navigation sidebar with icons for Home, Scan, Update, Web protection (selected), Proactive, Logs, Whitelist, and Settings. The main area is titled 'Web protection' and contains a sub-menu with 'Categories', 'Application rules', 'Time restriction', and 'Keywords' (selected). Below this, there are input fields for 'URL / Keyword' and 'Description'. The 'Match source' section has radio buttons for 'URL' (selected), 'Content', 'IP', 'Downloads', and 'Uploads'. The 'Action' section has radio buttons for 'Block' (selected) and 'Allow'. A yellow 'Add' button is positioned to the right of the action options. Below these settings is a table with the following structure:

Keyword	Description	Type	Action
(Empty table body)			

At the bottom right of the table area are two yellow buttons: 'Select/Unselect all' and 'Delete'. At the very bottom of the window, it shows 'Valid until 18.09.2019' and a yellow 'License' button.

## 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.

The screenshot displays the 'Settings' window for 'Unistal PROTEGENT AV Cloud'. The left sidebar contains navigation options: Home, Scan, Update, Proactive, Logs, Whitelist, and Settings (selected). The main area is titled 'Settings' and lists several categories: Protection, Scanner, Update, USB, Scheduler, Logs, Notifications, Password, and License. The 'Protection' category is active, showing the following settings:

- Enable system protection:
- AV:
- Antispyware:
- Low-risk programs:
- Code emulations:
- Check files when they are opened or copied:

Under 'Realtime detection':

- Folders/Drives:  [Browse](#)
- Extensions:  [Browse](#)
- Files:  [Browse](#)

Scan options:

- Scan by extensions [Browse](#)
- Scan all files
- Scan network shares

Action on detected malware:  File size limit:  MB

Additional options:

- Enable cloud check
- Scan cloud reputation [Exclusions](#)

Buttons at the bottom: [Default](#), [Apply](#), [License](#) (Valid until 25.07.2019)

## 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.

**Unistal's PROTEGENT AV Cloud**

**Settings**

- Protection
- Scanner**
- Update
- USB
- Scheduler
- Logs
- Notifications
- Password
- License

Category	Quick scan	Full scan	Custom scan
AV	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Antispyware	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Antimalware	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Low risk programs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scan cookies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scan registry	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scan processes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scan archives	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enable rootkit detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Scan at lower priority	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

File size limit: 30 MB

Action on detections: Prompt me

USB Drive behaviour:

- Scan automatically
- Ask me for action
- Do nothing

Exclusion filters

- Files
- Folders
- Extensions

Scan all files  Scan by extensions [Browse](#)

- Advanced behaviour heuristics
- Recover hidden USB files
- Scan cloud reputation
- Enable cloud check

[Exclusions](#)

[Default](#) [Apply](#)

Valid until 25.07.2019 [License](#)

## 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.

**Unistal's PROTEGENT AV Cloud**

- Home
- Scan
- Update
- Proactive
- Logs
- Whitelist
- Settings

### Update

Update version:	Virus signature date:	Last update date:	
95814800	22.07.2019	23.07.2019	<a href="#">Update now</a>

### Application automatic updates

Last upgrade: Never [Check for upgrade](#)

Current version: 10.5.0.9

Check update every: 1 day

### Full update packages(for manual download)

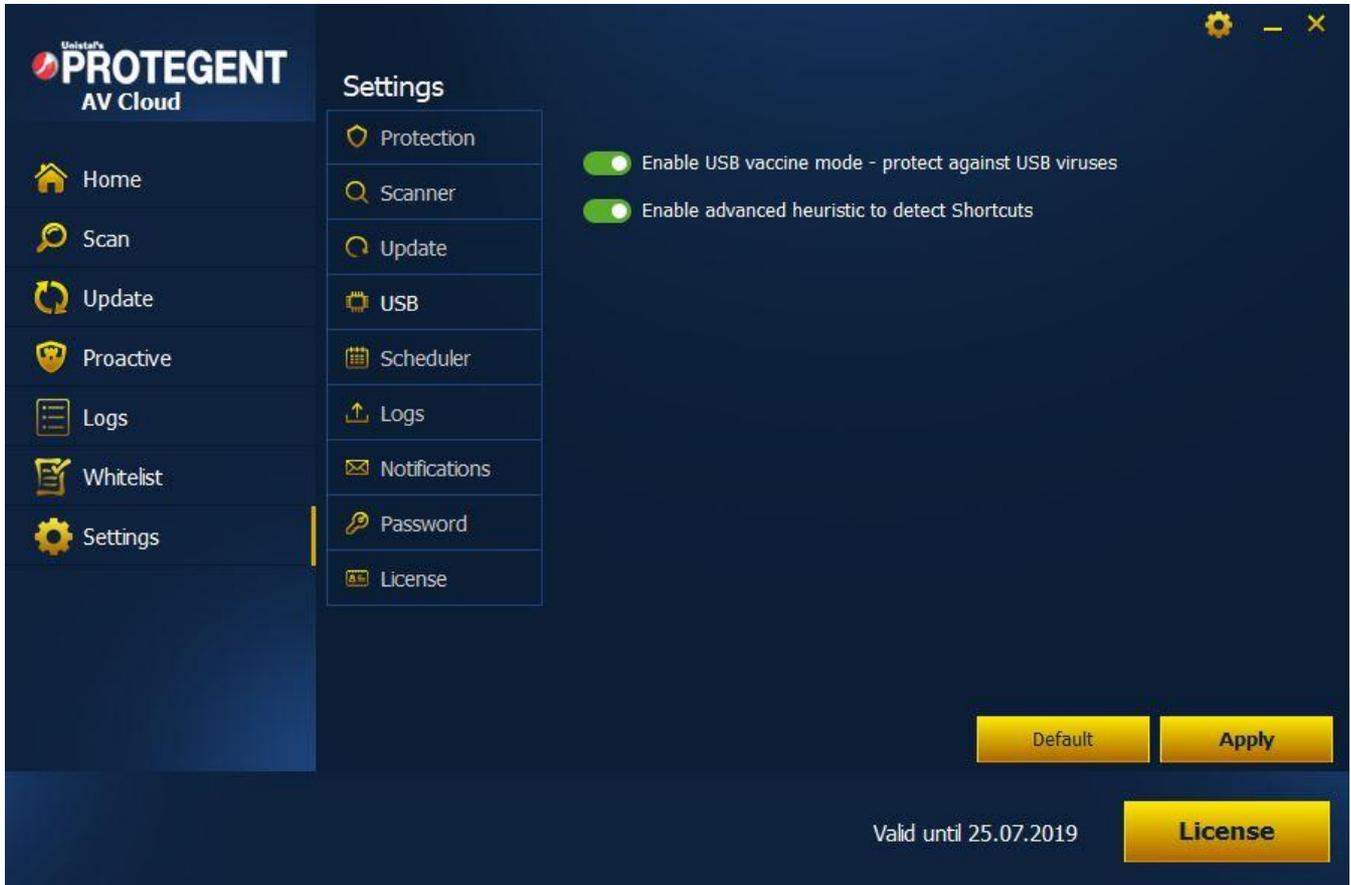
[Primary download server](#)

[Secondary download server](#)

Valid until 25.07.2019 [License](#)

## 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.

The screenshot displays the 'Scheduler' settings window within the Unistal's PROTEGENT AV Cloud interface. The window has a dark blue theme with yellow accents. On the left is a navigation sidebar with icons for Home, Scan, Update, Proactive, Logs, Whitelist, and Settings. The 'Settings' menu is open, showing options for Protection, Scanner, Update, USB, Scheduler, Logs, Notifications, Password, and License. The 'Scheduler' option is selected. The main content area is titled 'Settings' and contains the following configuration options:

- Configure the scan schedule so that you can run the different types of scan according to your settings**
  - Enable scheduled scan
- Week days**
  - Sunday  Monday  Tuesday  Wednesday
  - Thursday  Friday  Saturday
  - Time: 12:00:00 AM
- Scan type**
  - Quick scan  Full scan
- Scheduled scans action**
  - Automatically take the recommended cleaning action(Default action)
  - Show me the results and let me decide

At the bottom right of the settings area are two yellow buttons: 'Default' and 'Apply'. At the bottom of the window, there is a license status bar showing 'Valid until 25.07.2019' and a yellow 'License' button.

## 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.

The screenshot displays the Unistal's PROTEGENT AV Cloud interface. On the left is a dark blue sidebar with the following menu items: Home, Scan, Update, Proactive, Logs (highlighted with a yellow bar), Whitelist, and Settings. The main content area has a dark blue background and features a table with the following headers: Select, Date & time, Object path, Threat name, Risk level, Action taken, and Malw. Below the table is a horizontal scrollbar. At the bottom of the main area, there is a 'Select Logs:' dropdown menu currently set to 'Protection Logs', followed by three yellow buttons: 'View logs', 'Select/Unselect all', and 'Clear logs'. In the bottom right corner, there is a license status 'Valid until 25.07.2019' and a yellow 'License' button.

## 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.

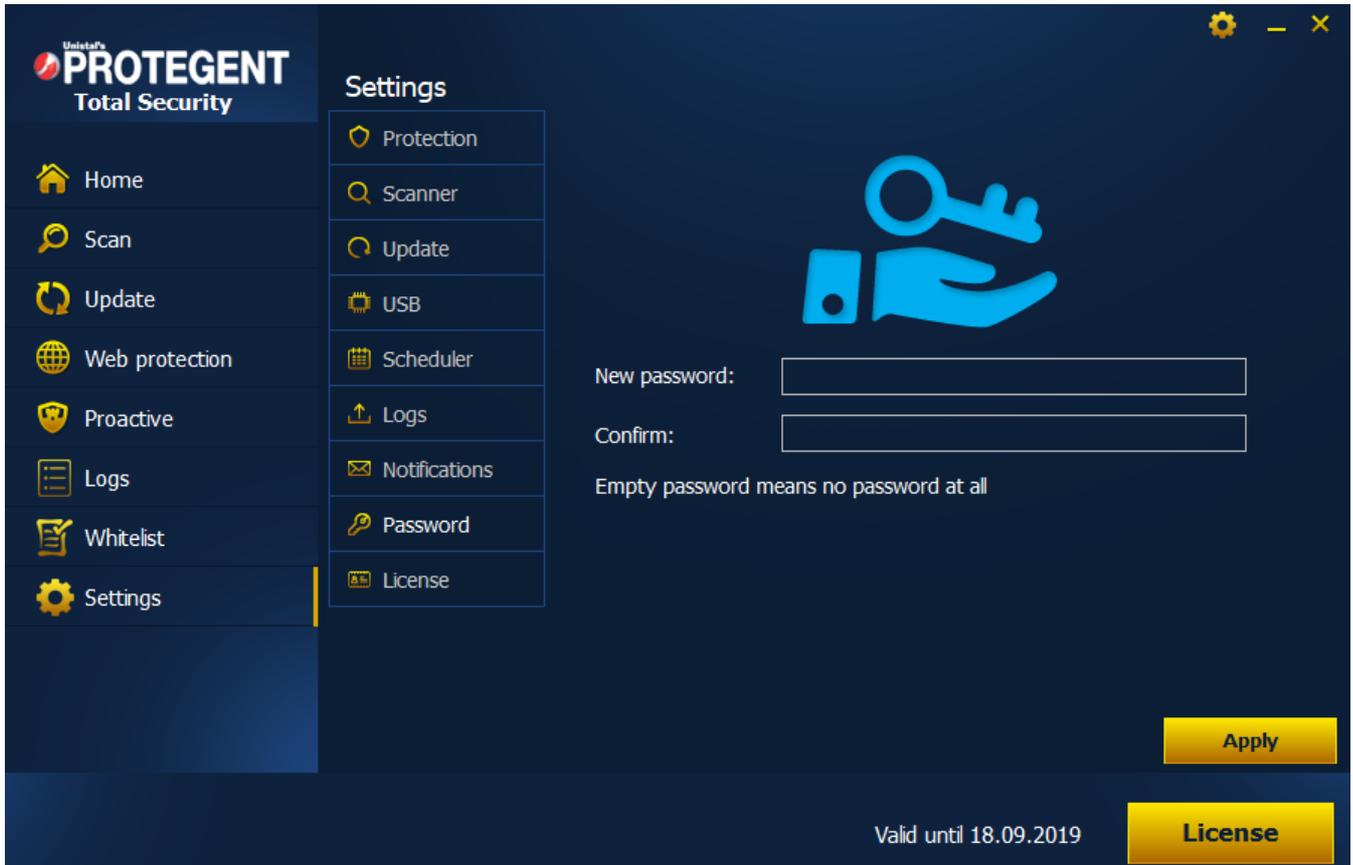
The screenshot shows the 'Settings' window for Unistal's PROTEGENT Total Security. The 'Notifications' tab is selected in the left-hand menu. The main area displays the following settings:

- Notifications settings define how customers are notified about product security events**
- Settings:**
  - Real-time virus alert:
  - Scan alert:
  - Update alert:
- Display balloon tips in taskbar for:** 10 seconds

At the bottom right, there are three buttons: 'Default', 'Apply', and 'License'. The 'License' button is highlighted. Below the 'License' button, it says 'Valid until 18.09.2019'.

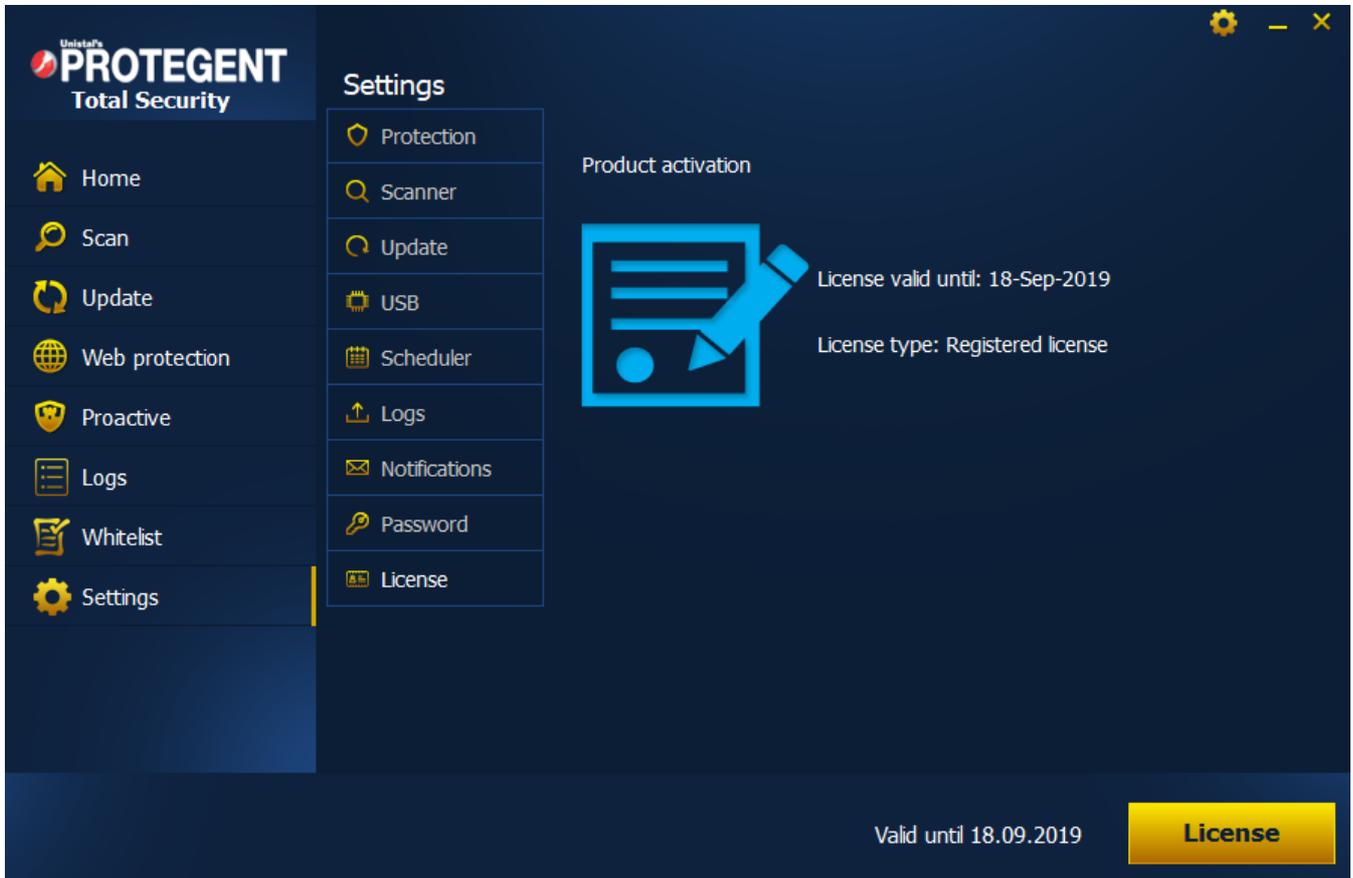
## Password

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



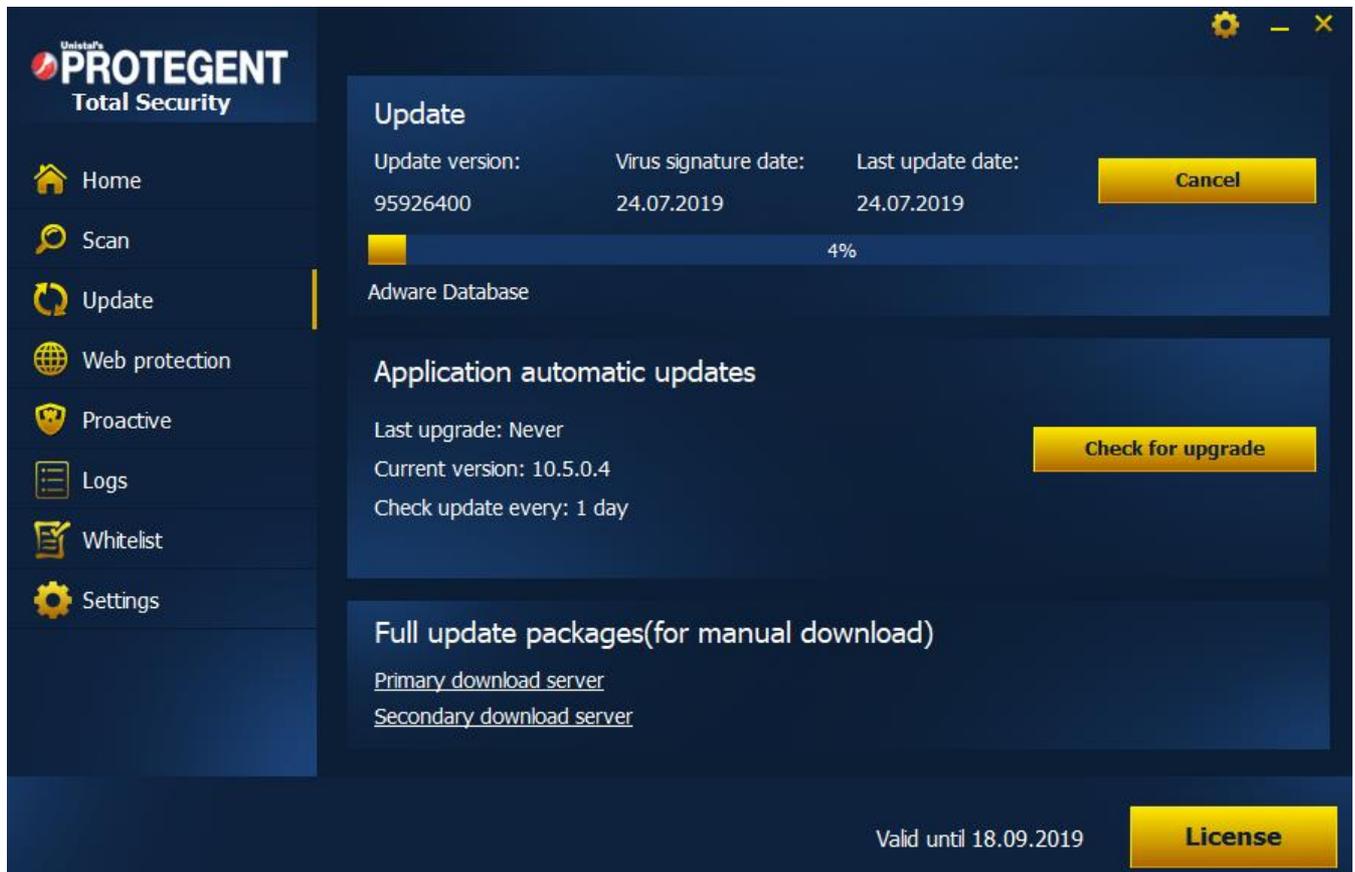
## License

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.

License Registration
✕

Username:	Password:
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="password"/>
First name:	Last name:
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
Company (optional):	Phone number:
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
Email address:	Country:
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text" value="India"/>
State:	District:
<input style="width: 95%;" type="text" value="ANDAMAN &amp; NICOBAR ISLANDS"/>	<input style="width: 95%;" type="text" value="NICOBAR"/>
Note (optional):	
<input style="width: 98%;" type="text"/>	
-----	
Dealer name (optional):	Dealer firm (optional):
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
Dealer mobile (optional):	Dealer email (optional):
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
Dealer address (optional):	Dealer (optional):
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text" value="Distributor"/>

I would like to receive product news and special offers

OK
Cancel

## 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.

**Protegent Total Security**

Definitions version: 95926400  
 Definitions date: 24.07.2019  
 Version: 10.5.0.4

Email:  
[isales@unistal.com](mailto:isales@unistal.com) (Sales)  
[support@unistal.com](mailto:support@unistal.com) (Support)

**Unistal Systems Pvt. Ltd.**  
 For Support Call Toll Free:  
 1800 102 5400 (Only For India)

[Buy license](#)   [Surrender license](#)   [Close](#)

## 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

Select	Date & time	Update status	Update source	Virus signature
<input type="checkbox"/>	2019-07-24 15:41:12	Success	Global	95926400(24.07.2019)
<input type="checkbox"/>	2019-07-24 15:35:16	Success	Global	95926400(24.07.2019)

Select Logs: Update Logs Protection Logs **Scanner Logs** Update Logs Event Logs Quarantine

[View logs](#)   [Select/Unselect all](#)   [Clear logs](#)   [License](#)

Valid until 18.09.2019

## 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.

The screenshot displays the 'Quarantine' section of the Unistal Protegent Total Security software. On the left is a dark blue sidebar with the 'PROTEGENT Total Security' logo and navigation icons for Home, Scan, Update, Web protection, Proactive, Logs, Whitelist, and Settings. The main window features a table with the following headers: 'Select', 'Date & time', 'Threat name', 'Path', and 'No of traces'. Below the table is a horizontal scrollbar. At the bottom of the main area, there are four yellow buttons: 'Select/Unselect all', 'Remove from quarantine', 'Restore quarantine', and 'Restore quarantine to'. Below these buttons is a 'Select Logs:' label followed by a dropdown menu currently showing 'Quarantine' and a 'View logs' button. In the bottom right corner, the text 'Valid until 18.09.2019' is displayed next to a yellow 'License' button.

## WHITELIST

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

**Unistal's PROTEGENT Total Security**

**Whitelist**

No files configured to be excluded from Realtime and Manual malware scanning

Select	File path

Refresh    Select/Unselect all    Delete    Add file

Valid until 18.09.2019    License

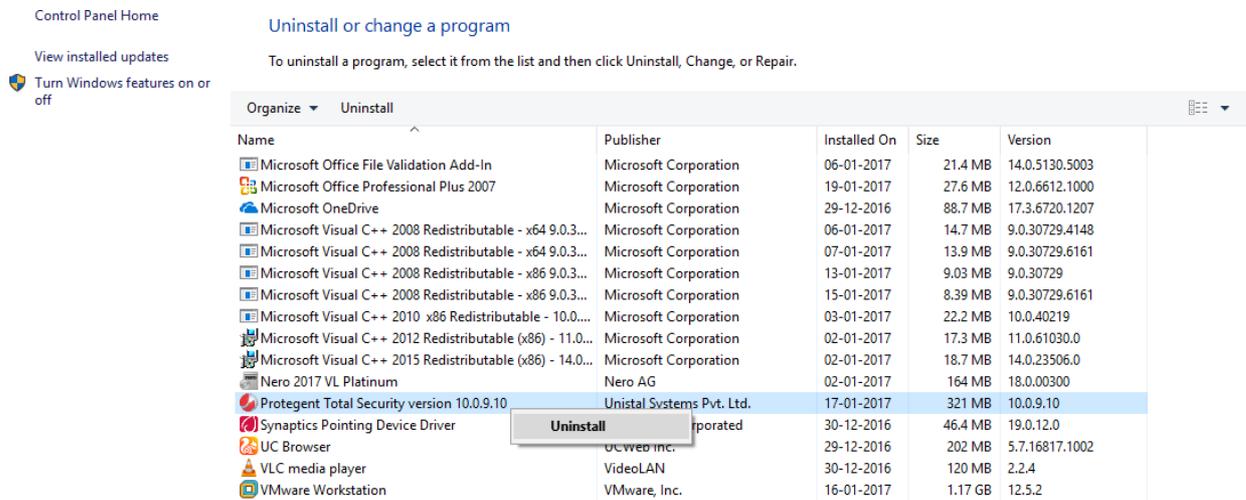
## UNINSTALLING PROTEGENT TOTAL SECURITY

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

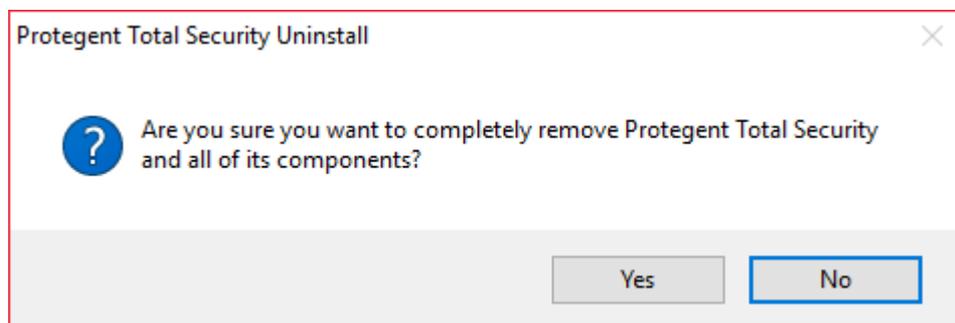
- In control Panel screen, click on **Uninstall a program** option



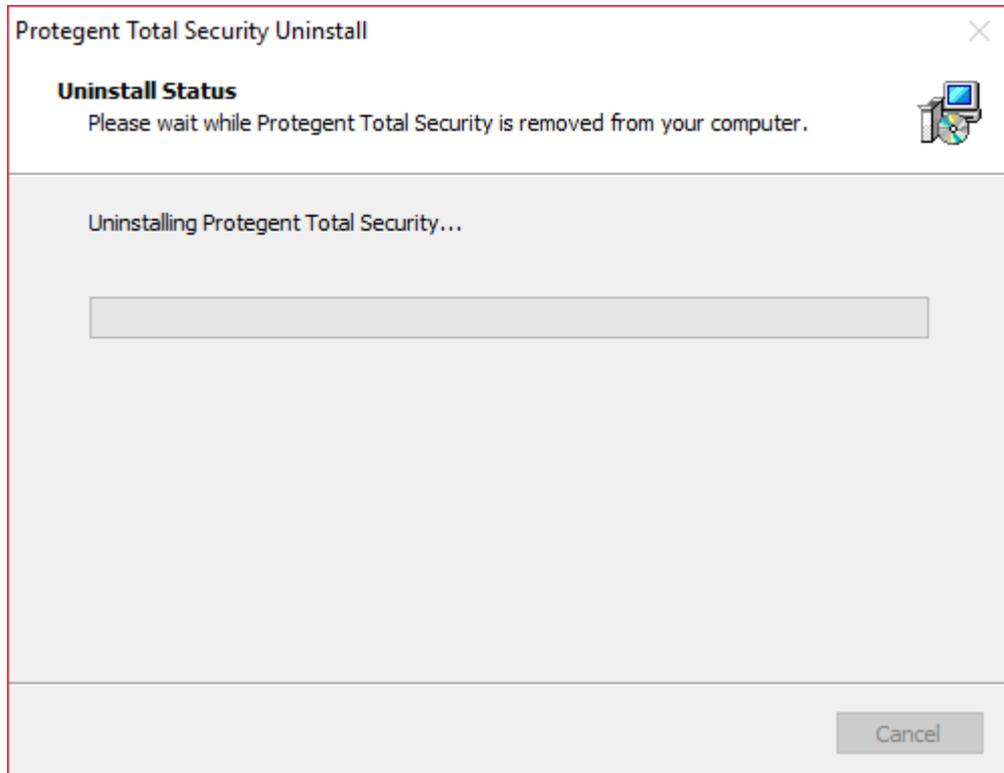
- This will navigate you to a list of the system programs that you have installed. Select “Protegent Total Security Version” program and right click. It will then show you the option to uninstall the program as shown in the image.



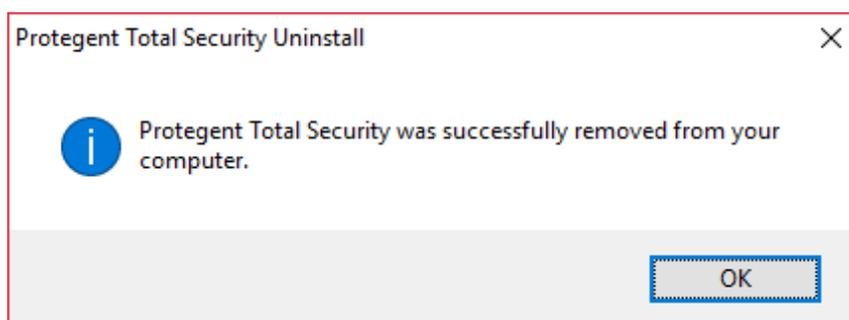
- Click on “Un-install” and follow the process to un-install.
- One dialogue box will appear where it will ask for the last time “Are you sure you want to completely remove Protegent Total Security and all of its components”



- 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<sup>®</sup>

Products, please visit <http://protegent360.com/>

No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from Unistal<sup>®</sup>.

Sales: [isales@unistal.com](mailto:isales@unistal.com)

Support: [support@unistal.com](mailto:support@unistal.com)

Website:

<http://protegent360.com/>