



Antivirus

User Guide

Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in CloudActiv8's "Click-Accept" EULA as updated from time to time by CloudActiv8 at <http://www.CloudActiv8.com/legal.aspx>. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from CloudActiv8 as continued use of the Software or Services indicates Customer's acceptance of the Agreement."



Contents

Show	Error! Bookmark not defined.
Machines	6
Dashboards	14
Detections	14
Configuration	16
Profiles	16
Alerts	34
Settings	37
Administration	40
Application Logging	40



Antivirus Overview

Antivirus provides Kaspersky Antivirus endpoint security for managed machines. **Antivirus** ensures protection of your computer against known and new threats. Each type of threat is processed by separate application components, each of which can be enabled or disabled by configuration profile. Configuration profiles enable you to quickly apply different types of **Antivirus** solutions to many machines at the same time. **Antivirus** can be installed independently of **Endpoint Security** or *Anti-Malware (Classic)*.

Antivirus includes the following protection tools:

- Memory-resident protection components for:
 - Servers and workstations, with separate licensing for each
 - Files and personal data
 - System
 - Network
- Scheduled, recurring virus scans of individual files, folders, drives, areas or the entire computer.
- Updates of the **Antivirus** clients and its components, as well as the **Antivirus** definition databases used to scan for malicious programs.
- Status dashboard for all **Antivirus** managed machines.
- A Detections page for all virus threats not automatically resolved by **Antivirus**.
- Module managed alerts.
- Windows Security Center checking.
- An Antivirus Upgrade Recommended filter helps you identify out-of-date **Antivirus** clients.
- **Policy Management** can manage the installation of the **Antivirus** client and the assignment of **Antivirus** profiles and alert profiles.
- A Settings page enables to you specify global exclusions that can be optionally added to any profile. You can also make profiles public or private.
- Peer-to-peer file downloading automatically fetches **Antivirus** install files from other endpoints on the same local network, if these files have already been downloaded.
- Peer-to-peer file downloading of Kaspersky definition files using **Use LAN Updater** and LAN Cache is also provided.



Functions	Description
Machines	Installs and uninstalls Antivirus software on selected machines and provides a detailed view of the Antivirus status of any selected machine.
Dashboards	Displays a dashboard view of the status of all machines installed with Antivirus.
Detections	Displays virus threats you can take action on.
Profiles	Manages Antivirus profiles that are assigned to machine IDs.
Alerts	Manages Antivirus module alerts.
Settings	Maintains module-level preferences.
Application Logging	Displays a log of Antivirus module activity.

Antivirus Module Minimum Requirements

Antivirus R95 requires agent version 9.3.0.0 or higher. Requirements for Each Managed Workstation

- 1 GHz CPU or greater
- 1 GB available RAM
- 2 GB free space on the hard drive
- Microsoft Windows 7, 8, 8.1, 10 are supported.
- Microsoft

Windows Installer 3.0
Requirements for
Each Managed Server

- Server 2008 SP1, SBS 2008 SP1, 2008 R2 SP1, SBS 2011, 2012, 2012 R2, 2016 are supported.
- Only the OS of SBS 2011 is supported. It does not include Exchange email servers hosted by SBS 2011.

See *Kaspersky Endpoint Security 10 for Windows (for workstations)*, version v10.3.0.6294 for a complete list of workstation system requirements.

See **Kaspersky Endpoint Security for Windows, version v10.3.0.6294**

for a complete list of server system requirements,
including service pack requirements for each OS.

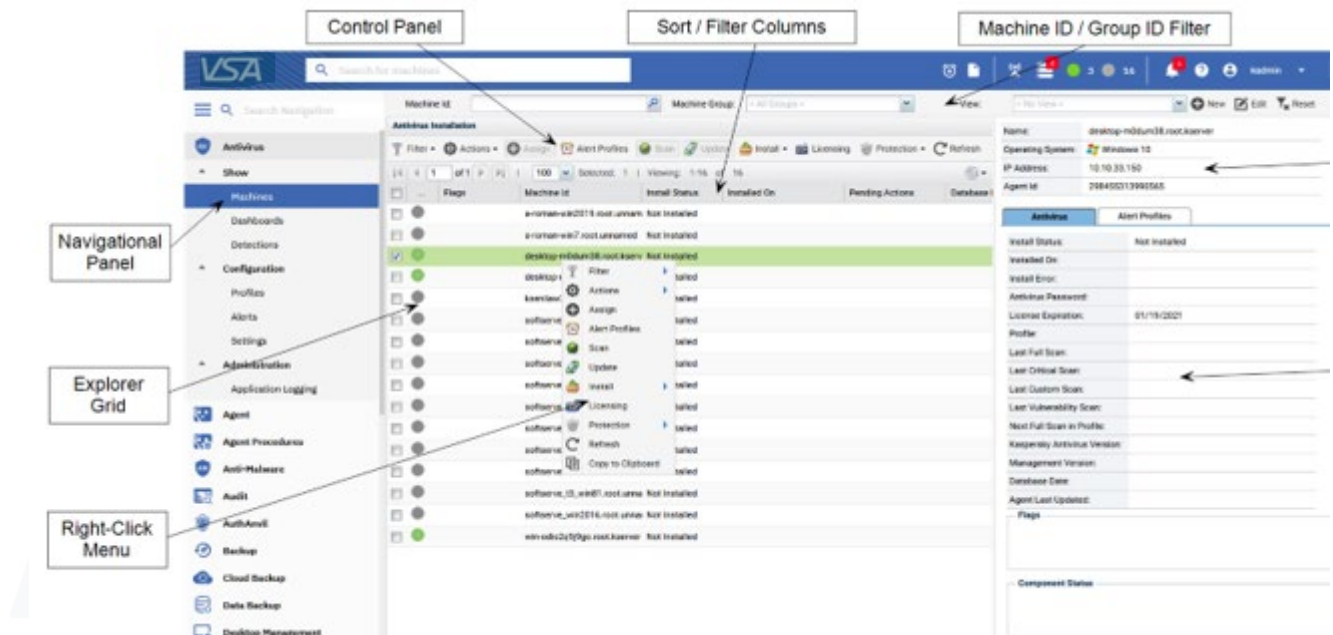
Machines

Antivirus > Show > Machines

The **Machines** page installs and uninstalls **Antivirus** software on selected machines. This same page also provides a detailed view of the **Antivirus** status of any selected machine.

Page Layout

The layout of the **Machines** page comprises the following design elements:

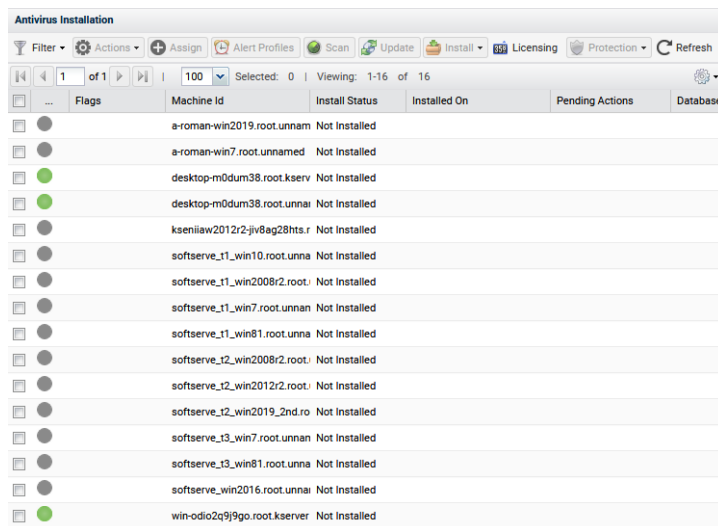


- **Navigational Panel** - Used to navigate to pages within the **Antivirus** module.
- **Explorer Grid** - Each managed machine in the CloudActiv8 is listed in this panel.
 - **Page Browser** - If more than one page of devices displays, pages forwards and back.
 - **Rows Per Page** - Sets the number of devices displayed per page: 10, 30 or 100.
- **Machine ID / Group ID Filter** - Filters the list of machines ID listed in the **Explorer Grid**.
- **Control Panel** - Executes tasks, either for the entire **Explorer Grid** or for a single selected machine.
- **Details Panel** - This panel displays the properties and status of a single machine.
 - **Header** - Identifies the selected machine in the **Explorer Grid**.
 - **Antivirus** - Displays a summary of the **Antivirus** status of a machine.
 - **Alert Profiles** - Lists the alert profiles assigned to a machine.
- **Right Click Menu** - Selects actions for row using a right click menu.
- **Sort / Filter Columns** - Click the header of any column to sort or filter columns.

Explorer Grid

The **Explorer Grid** of the **Machines** page lists all agent machines your current scope and **machine ID / group ID filter** permit you to see. Additional columns display information about machines installed with **Antivirus**.







- Page forward displays multiple pages of machines.
- Machines per page sets the number of rows on each page.



Flags	Machine Id	Install Status	Installed On	Pending Actions	Database
	a-roman-win2019.root.unnam	Not Installed			
	a-roman-win7.root.unnamed	Not Installed			
	desktop-m0dum38.root.kserv	Not Installed			
	desktop-m0dum38.root.unnai	Not Installed			
	ksenilaw2012r2-jiv8ag28hts.r	Not Installed			
	softserve_t1_win10.root.unna	Not Installed			
	softserve_t1_win2008r2.root.	Not Installed			
	softserve_t1_win7.root.unnan	Not Installed			
	softserve_t1_win81.root.unna	Not Installed			
	softserve_t2_win2008r2.root.	Not Installed			
	softserve_t2_win2012r2.root.	Not Installed			
	softserve_t2_win2019_2hd.ro	Not Installed			
	softserve_t3_win7.root.unnan	Not Installed			
	softserve_t3_win81.root.unna	Not Installed			
	softserve_win2016.root.unnai	Not Installed			
	win-odio2q9j9go.root.kserver	Not Installed			

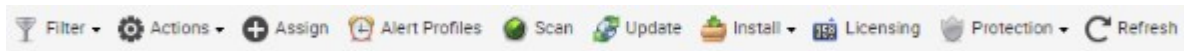
Component Icon Conventions

Hovering the mouse over a component icon displays a tool tip describing the status of the component. In general, the following component icon conventions are used.

Status	Type of Icon Displayed	Example: File Protection Icons
Disabled	grey X mark	
Failure	yellow exclamation point	
Running/Enabled	green checkmark	
Starting	a key with a green arrow	
Stopped	red X mark	
Stopping	a key with a red minus sign	

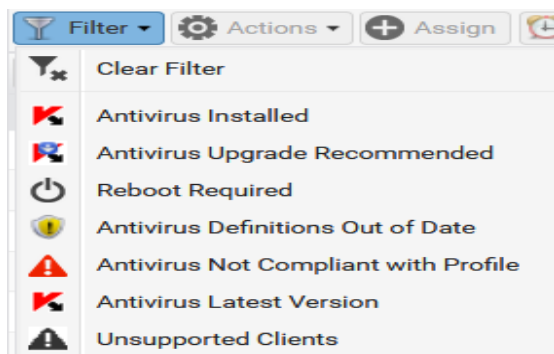
Control Panel

The **Control Panel** at the top of the Machines page executes tasks, either for the entire Explorer Grid or for a single selected machine.



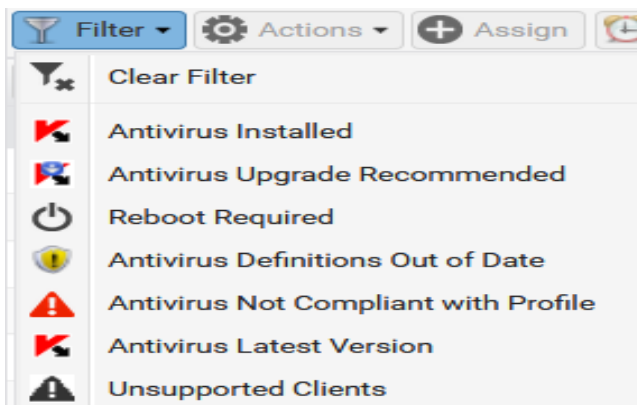
Filter

Filters the list of rows displayed. A filter icon displays in the **Flags** column when a filter is set.



- **Clear Filter** - Clears the grid of any selected filters.
- *Antivirus Installed*
- **Antivirus Upgrade Recommended** - Helps you identify which machines are eligible for upgrading to the latest version. To upgrade, install over an existing installation of **Antivirus (Classic)**.
- *Reboot Required*
- **Antivirus Definitions Out of Date**
- **Antivirus Not Compliant with Profile**
- **Antivirus Latest Version**
- **Unsupported Clients**
- **Export** - Exports the grid to a CSV file.
- **Refresh** - Refreshes the grid.
- **Reset Filter** - Clears the grid of any selected filters

Gear



Actions

- **Cancel Pending Action** - Cancels pending actions on selected machines.
- **Reboot** - Reboots selected machines.

Clear Pending Action Errors - Clears pending error icons displayed in the user interface.

Assign

Assigns a **Antivirus** configuration profile to selected machines. Workstations and servers can be selected and assigned at the same time. You do not have to select only workstations or only servers. Workstations are assigned the selected workstation profile. Servers are assigned the selected server profile. See Profiles for more information.

Alert Profiles

Assigns or removes an alert profile for selected machines. The **Alert Profiles** tab on the Details Panel displays all profiles assigned to a machine.

Scan

Schedules an **Antivirus** scan on selected machines.

- **Start Date/Time** - The start date and time of the scan. For **Antivirus** there are four types of scan:
 - **Critical Scan** - Virus scan of operating system startup objects. Quick Scan was renamed to Critical Scan starting with **Antivirus** version 10.x.
 - **Full Scan** - A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
 - **Custom Scan** - Scans unprocessed files. An infected file is considered unprocessed if no action—such as disinfect, delete, or block—was taken while scanning the computer for viruses and other threats.
 - **Vulnerability Scan** - Virus scan of operating system startup objects.

Update

Schedules an update on selected machines with the latest **Antivirus** definitions. Also, activates the Kaspersky license on the machine, if the license was removed or never installed correctly.

- **Start Date/Time** - The start date/time of the update.

Install

- **Install or Upgrade Antivirus** - Installs or upgrades the **Antivirus** client on selected machines to version 10.3.0.6294. Version 10.2.5.3201 and 10.2.4.674 installs continue to be supported. This includes taking over management of machines that already have Kaspersky Endpoint Security for Business, version 10.2.4.674 installed, independently of the CloudActiv8.
 - **Profile Selection** - Select the profile to be applied. Workstations and servers can be selected and installed at the same time. Workstations are assigned the selected workstation profile. Servers are assigned the selected server profile. Only version 10.x workstation and server profiles can be selected.
 - **Advanced Options**
 - ✓ **Start Date & Time** - The start date and start time of the install.
Prompt before install - If checked, the Installation only proceeds if the user is logged on and agrees to proceed.
 - ✓ **Password** - Sets a custom password to use with this machine. Passwords prevent an unauthorized uninstall or reconfiguration. Leave blank to use the default password. The default password is used when installing **Antivirus** using **Policy Management**. The password displays in the Details Panel. Passwords must be alphanumeric. Special characters are not supported.
 - ✓ **Blocking Install Issues** - Lists issues that can prevent a successful installation on selected machines.
- **Uninstall Antivirus** - Uninstalls the **Antivirus** client on selected machines.
 - **Start Date & Time** - The start date and start time of the uninstall.
- **Repair Antivirus Install** - Re-installs missing files on a previously installed **Antivirus** client to repair it. The **Antivirus** client must have been previously installed using the same CloudActiv8.
 - **Start Date & Time** - The start date and start time of the repair.

Licensing

Licensing sets the expiration date for all **Antivirus**, **Anti-Malware**, and **Endpoint Security** client licenses purchased equal to the CloudActiv8 maintenance expiration date.

- **License Counts** - Lists **Antivirus** license counts for servers and workstations. Licenses for servers and workstations are purchased and tracked separately. **Antivirus** license counts also display on the Administration > Manage > **License Manage**
 - **Total Purchased to date**
 - **Full Available** (Purchased not applied or expired)
 - **Applied** (Active license applied to a machine)
 - **Expiration Date**
 - **# of Days Remaining** - Days remaining before all licenses expire.



Protection

- **Get Status** - Returns the enable/disabled status of **Antivirus** components on a machine and, if necessary, corrects the display of the component status icons in the **Explorer Grid**. Also returns the install and database signature version information.
- **Temporarily Enable Antivirus** - Re-enables **Antivirus** protection on selected machines.
- **Temporarily Disable Antivirus** - Disables **Antivirus** protection on selected machines. Some software installations require **Antivirus** software be disabled to complete the install.
- Exporting

Columns

All columns support **selectable columns**, **column sorting**, **column filtering** and **flexible columns widths**

Selectable Columns

- **Agent Id** - The unique GUID of the CloudActiv8 agent, in string format.
- **Flags** - Possible flags include: Definitions out of date
- **Machine ID** - A unique machine ID / group ID / organization ID name for a machine in the CloudActiv8.

Install Status

Not Installed, Script Scheduled, Installed, Installed (Classic AV)

- **Installed On** - The date **Antivirus** was installed.
- **Pending Actions** - Install, Assign, Update, Scan. Clicking the pending action icon during an install displays the following action statuses: **Downloading File**, **Installing**, **Downloading OEM files to the CloudActiv8**, **Downloading Files to the endpoint**, **Installing product on the endpoint**.
- **Database Date** - The date the definition database was last updated.
- **Kaspersky Antivirus Version** - The version number of the Kaspersky client installed on this machine. (R)
- **WSC Reported Product Name** - The name of the security product registered with *Windows Security Center*.
- **AV Components** - Identifies the status of **Antivirus** components installed on this machine.
- **AV Profile** - The **Antivirus** profile assigned to this machine.
- **Has Active Threats** - Number of detections that could not be automatically disinfected or deleted and require user attention.
- **Last Critical Scan** - The last date and time a critical area scan of operating system startup objects was performed.

- **Last Custom Scan** - The last date and time a custom scan is scheduled to be performed.
- **Last Full Scan** - The last date and time a thorough scan of the entire system was performed. Includes: system memory, programs loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Last Reboot** - The date/time the machine was last rebooted.
- **Last Vulnerability Scan** - The last date and time a vulnerability scan is scheduled to be performed.
- **Login Name** - The currently logged on user.
- **Management Version** - The version of the CloudActiv8 agent.
- **Next Full Scan** - Calculates the next full scan from the scheduled tasks section of the assigned profile.
- **Operating System** - The operating system of the machine.
- **Reboot Needed** - If Yes, a reboot is required.
- **Time Zone Offset** - Displays the number of minutes. See System > User Settings > **Preferences**
- **WSC Manufacturer** - The manufacturer of the WSC reported product.
- **WSC Up To Date** - If checked, the WSC reported product is up to date.
- **WSC Version** - The WSC reported product version.

Details Panel

Header

- **Name** - The machine ID.group, ID.organization, ID of the machine.
- **Operating System** - The operating system of the machine.
- **IP Address** - The IP address of the machine.
- **Agent Id** - The GUID of the agent on the managed machine.

Status tab

- **Install Status** - Not Installed, Script Scheduled, Installed
- **Installed On** - The date **Antivirus** was installed.
- **Install Error** - If an install error occurs, displays a description of the error.
- **Antivirus Password** - The password required to reconfigure or uninstall the Kaspersky client.
- **License Expiration** - The date **Antivirus** security is scheduled to expire.
- **Profile** - The **Antivirus** configuration **profile** assigned to this machine.
- **Last Full Scan** - The last date and time a thorough scan of the entire system was performed. Includes: system memory, programs loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Last Critical Scan** - The last date and time a critical area scan of operating system startup objects was performed.
- **Last Custom Scan** - The last date and time a custom scan is scheduled to be performed.
- **Last Vulnerability Scan** - The last date and time a vulnerability scan is scheduled to be performed.
- **Next Full Scan in Profile** - Calculates the next full scan from the scheduled tasks section of the assigned profile.
- **Kaspersky Antivirus Version** - The version number of the Kaspersky client installed on this machine.

- **Management Version** - The version of the CloudActiv8 agent.
- **Database Date** - The date and time of the **Antivirus** definition database currently being used by this machine.
- **Agent Last Updated** - The date and time the **Antivirus** client was last updated.
- **Flags** - Possible flags include: Virus definitions out of date, Configuration is out of compliance with the profile.
- **Component Status** - Identifies the status of **Antivirus** components installed on this machine. Component protection is specified using the Profiles > **Protection** tab.



-File - If checked, scans all files that are opened, saved, or executed.



- Web - If checked, ensures security while using the Internet. It protects your computer against data coming into your computer via the HTTP protocol, and also prevents dangerous scripts from being executed on the computer.



- Mail - If checked, scans incoming and outgoing messages for the presence of malicious objects. It is launched when the operating system loads, is located in computer RAM and scans all email messages received via the POP3, SMTP, IMAP, MAPI and NNTP protocols.



- IM - If checked, ensures safe operation of IM clients. It protects the information that comes to your computer via IM protocols. The product ensures safe operation of various applications for instant messaging, including ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent and IRC.



- Network Attack Blocker - If checked, inspects inbound network traffic for activity that is typical of network attacks. On detecting an attempted network attack that targets your computer, network activity is blocked from the attacking computer.




- System Watcher - Records application activity on the computer and provides this information to other components to ensure more effective protection.


Alert Profiles tab

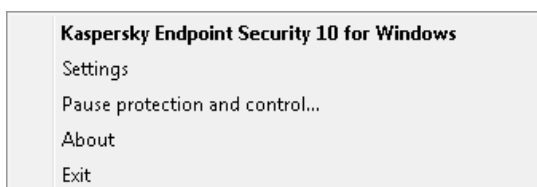
Displays the list of **alert profiles** assigned to the selected machine.

Antivirus Agent Menu



Once installed on a machine, a Kaspersky icon  displays in the computer's system tray. This icon provides access to the Kaspersky Endpoint Security user interface. Right clicking the Kaspersky icon

 displays an option menu.



- **CloudActiv8 Antivirus** - Displays the *Protection and Control* tab of the Kaspersky Endpoint Security user interface.
- **Settings** - Displays the *Settings* tab of the Kaspersky Endpoint Security user interface.
- **Pause protection and control...** - Pauses protection on the machine for a specified time period.
- **About** - Displays the *About* box for Kaspersky Endpoint Security.
- **Exit** - Terminates the Kaspersky Endpoint Security user interface only. Kaspersky continues to run in the background.

Dashboards

Antivirus > Show > Dashboards

The **Dashboards** page provides a dashboard view of the status of machines installed with **Antivirus**. The dashboard statistics displayed depends on the **machine ID / group ID filter** and machine groups the user is authorized to see using System > **Scopes**

Antivirus Protection Status - A pie chart displays percentage categories of machines with **Antivirus** protection. Percentage categories include **Not Installed**, **Out of Date**, **Not Enabled**, and **Up to Date**.

- **Antivirus Top Threats** - Lists the machines with the greatest number of threats. Clicking a hyperlinked machine ID displays the threats belonging to that machine ID in the **Detections** page.
- **Antivirus Unfiltered License Summary** - A chart displays the number of machines that are Available, Expired, In Use, Partials and Pending Install.
- **Antivirus Machines Needing Attention** - A bar chart displays the number of **Antivirus** managed machines needing attention, by category. Categories include No AV Installed, Uncured Threats, Out of Date, Reboot Needed, Component.
- **Antivirus Number of Machines with Detections** - A bar chart displays the number of detections.

Detections

Antivirus > Show > Detections

The **Detections** page displays virus threats not automatically resolved by **Antivirus**. Use the information listed on this page to investigate threats further and manually remove them. The list of machines displayed depends on the **machine ID / group ID filter** and machine groups the user is authorized to see using System > **Scopes**

Actions

- **Details** - Click to learn more about a selected threat from Kaspersky's Secure list web site.
- **Add Exclusion** - Adds selected rows to the **excluded** list.
- **Delete** - Sends a request to the endpoint to delete the quarantined file.
- **Restore** - Sends a request to the endpoint to remove the file from quarantine. The file is no longer considered a threat.
- **Hide** - Do not show in this list. Hiding does not delete the threat.
- **Filter** - Filters the list by one of the following:
 - **Active Threats** - Displays **Antivirus** threats that have been detected but not yet disinfected, deleted or excluded.
 - **Quarantined Files** - Displays quarantined files.
 - **Deleted Files** - Displays a list of deleted files.
 - **Threats Last <N periods>** - Filters the list by one or several predefined time periods.
 - **Clear Filter** - Removes all filtering from the list.

Table Columns

- **Machine Name** - The machine ID.
- **Name** - The name of the threat.
- **Path** - The location of the threat on the managed machine.
- **Time** - The date and time the threat was detected.
- **Status** - The status of the threat. Status messages include but are not limited to:
 - **Infected** - File was found to be infected with a virus.
 - **Suspicious** - File is suspicious. Usually this means malware but is not a confirmed, known virus.
 - **Disinfected** - Kaspersky cleaned the virus from the file.
 - Deleted**
 - File was deleted, either automatically or after it was in quarantine.
 - **Quarantined** - File is in quarantine, cannot be accessed by the user but can be restored or deleted. To restore a quarantined file, use the password displayed for a machine in the Machines > **Details Panel**
 - **Detected** - Kaspersky made a detection but no action was taken: not quarantined, deleted, etc. This can potentially be an active threat. User needs to process the threat using options available in **Manage Detection**.
 - **Not Found** - The file no longer exists. It may have been deleted after it was detected, but it wasn't deleted by Kaspersky. This can occur when a temporary file is found, for example a cookie or temp file, that has already been deleted by deleting the browser cache.

- **Unknown** - The file is not recognized by Kaspersky's virus definitions. If further investigation is required, create a CloudActiv8 **support ticket**
- **RemediatedByUser** - The file was handled manually by the user. In this case, the user got a pop-up asking if they wish to delete/quarantine/ignore this threat and the user took the action on their own.
- **Type** - The category of threat.
- **Profile Name** - The name of the profile in use when this threat was detected.

Configuration

Profiles

Antivirus > Configuration > Profiles

The **Profiles** page manages **Antivirus** profiles. Each profile represents a different set of enabled or disabled **Antivirus** options. Changes to a profile affect all machine IDs assigned that profile. A profile is assigned to a machine ID when installing **Antivirus**, or by using Antivirus > **Machines** > **Assign** after the install. Typically different types of machines or networks require different profiles. Profiles are public by default. Use the Settings > **Application Settings** tab to make profiles private.





Profile Types - Servers and Workstations

Antivirus licenses are purchased and tracked separately for servers and workstations. Each are assigned separate types of profiles. A server profile can only be assigned to servers. A workstation profile can only be assigned to workstations. System profiles of each profile type are provided for you. System profiles cannot be deleted or edited. Workstations and servers can be selected and assigned at the same time.

Actions

- **New** - Creates a new configuration profile. Each type of profile installs a different type of client on the endpoint. Types of profile include:
 - **Kaspersky Workstation 10 Profile**
 - **Kaspersky Server 10 Profile**
- **Edit** - Edits an existing profile. You can also double-click a profile to open it.
- **Delete** - Deletes an existing profile.
- **Copy** - Saves a selected profile with new name. Server profiles can only be copied to a new server profile. Workstation profiles can only be copied to a new workstation profile.

Table Columns

- **(Created by)** -  (user) or  (system)
- **Name** - Name of the profile.
- **Description** - A description of the profile.
- **Profile Type** -  (server) or  (workstation)
- **Machines** - Number of machines using this profile.
- **Product Version** - 10.3.3.275 - Kaspersky Endpoint Security for Business, version 10
- **Created Date**
- **Last Updated By**
- **Last Updated**
- **Used in a Policy**

Profile Detailstab

Antivirus > Configuration > Profiles > New or Edit > Profile Details

The **Profile Details** tab sets header attributes for the profile.

- **Name** - The name of the profile.
- **Description** - A description of the profile.
- **Type** - **Antivirus** file server or workstation.
- **Security Level** - Three security levels are provided:
 - **High** - Set this level if you suspect a computer has a high chance of being infected.
 - **Recommended** - This level provides an optimum balance between the efficiency and security and is suitable for most cases.
 - **Low** - If machine operates in a protected environment low security level may be suitable. A low security level can also be set if the machine operates with resource-consuming applications.
 - **Custom** - Enables every option to be set individually. The entire profile is set automatically to Custom if a tab option is changed from its Low, Recommended or High default value.

Protection tab

Options tab

Antivirus > Configuration > Profiles > New or Edit > Protection > Options tab

- **Start Antivirus on Computer Startup** - If checked, all protection components selected for this profile are enabled at startup.
- **Enable Advanced Disinfection Technology** - Purges the operating system of malicious programs that have already started their processes in RAM and that prevent Kaspersky Endpoint Security from removing them by using other methods.

- Uses considerable operating system resources, which may slow down other applications.
- Requests the user's permission after completion to reboot a workstation.
- After the reboot, deletes malware files and starts a light full scan of the computer.
- **Show Icon In System Tray** - If checked, displays the **Antivirus Agent Menu** icon in the system tray. If unchecked, the icon is hidden. Changing this setting requires a reboot of the machine to take effect.
- **Monitor the following ports** - *Workstation profiles only*. Specifies the list of network ports monitored by the Mail Antivirus, Web Antivirus, and IM Antivirus components.

Objects for Detection tab

Antivirus > Configuration > Profiles > New or Edit > Protection > Objects for Detection

Malware

- **Viruses and Worms** - *Workstation profiles only*. A malicious software program that attempts to replicate itself on a computer. A worm does not need to attach itself to an existing program.
- **Trojan Programs** - *Workstation profiles only*. A malicious software program misrepresenting itself to appear useful, routine, or interesting to persuade a victim to install it.
- **Malicious Tools** - Software programs that have been designed to automatically create viruses, worms, or trojans.

Adware, Auto-Dialers, and Other Programs

- **Adware** - A software package that displays advertisements to the computer user, often without the user's permission or control.
- **Auto-Dialers** - A software program that attempts to dial telephone numbers, which can incur calling charges.
- **Other** - Remote administration utilities, which can be legitimate or installed by trojan programs for malicious purposes.



Compressed Files

- **Packed files that may cause harm** - Scans for antiviruses contained in compressed files, especially files using non-standard compression packages.
- **Multi-packed Files** - Scans files compressed multiple times in a nested fashion.

File Antivirus tab

Antivirus > Configuration > Profiles > New or Edit > Protection > File Antivirus

If enabled, **File Antivirus** remains active in memory and monitors all files that are opened, saved, or started on the computer and on all connected drives.

- **Enable Antivirus** - If checked, scans all files that are opened, saved, or executed.

Security Level

- *Security Level*
 - **High** - Set this level if you suspect a computer has a high chance of being infected.
 - **Recommended** - This level provides an optimum balance between the efficiency and security and is suitable for most cases.
 - **Low** - If machine operates in a protected environment low security level may be suitable. A low security level can also be set if the machine operates with resource-consuming applications.
 - **Custom** - When any other setting on this tab is changed, the **Security Level** is set to Custom. Reset the **Security Level** to High, Recommended or Low to reset options to their default settings.

Action on Threat Detection

- **Select action automatically** - If checked, automatically performs actions recommended by Kaspersky Lab. Once a threat is detected, the application attempts to disinfect the object. If disinfect fails, the application attempts to delete it. Suspicious objects are skipped without processing. If blank, protection uses the customized settings below.
- *Select Action*
 - **Disinfect** - If checked, an attempt is made to disinfect a quarantined file.
 - **Delete if disinfection fails** - If a quarantine file fails to be disinfected, it is deleted.
 - If both of the above are unchecked, the file is skipped, and the threat is added to the **Detections** page.

File Types

- *File Types*
 - **All files**
 - **Files Scanned by Format**
 - **Files Scanned by Extension**



Protection Scope

- **Protect Network Drives** - If checked, includes mapped network drives.
- *Protect Hard Drives* -
- **Protect Removable Drives** - If checked, includes removable drives.

Scan Methods

- **Heuristics Analysis** - If checked, uses heuristics analysis to identify the behavior of objects as malicious or suspicious, even if they are not yet identified as known threats in the signature database. This allows new threats to be detected even before they have been researched by virus analysts.
- **Depth** - Depth of heuristic analysis to use: Light, Medium, Deep.

Scan Optimization

- **Scan New and Changed Files Only** - If checked, scans only new files and files modified since the last scan.

Scan of Compound Files

- **Scan Archives** - If checked, scans archived files.
- **Scan Installation Packages** - If checked, scans installation packages.
- **Scan Objects** - If checked, scans office objects.
- **Extract Compound Files in the Background** - If checked, compound files larger than the size specified by **Minimum File Size (MB)** are extracted and scanned in the background while the user starts to work with the compound file. This eliminates the delay required to scan large compound files. Compound files include archives, installation files and embedded OLE objects.
- **Minimum File Size (MB)** - Specifies the minimum file size for background scanning of compound files.
- **Do Not Unpack Large Compound Files** - If checked, compound files larger than the size specified by **Maximum File Size (MB)** are not scanned. Files extracted from an archive are always scanned, regardless of this setting.
- **Maximum File Size (MB)** - Specifies the maximum file size for suppressing the scanning of files.



Scan Mode

- **Smart Mode** - Scan files after analyzing operations that are performed with the file by the user, by an application or by the operating system.
- *On Access and Modification*
- **On Access**
- **On Execution**

Scan Technologies

- **iSwift technology** - If checked, iSwift technology is used to speed up scans. Rescanning is ignored for previously scanned *NTFS objects* unless the object, scan settings, or antivirus database have changed.
- **iChecker technology** - If checked, iChecker technology is used to speed up scans. Rescanning is ignored for previously scanned *objects* unless the file, scan settings, or antivirus database have changed.

Mail Antivirus tab

Antivirus > Configuration > Profiles > New or Edit > Protection > Mail Antivirus

If enabled, **Mail Antivirus** scans incoming and outgoing email messages for viruses and other threats.

- **Enable Mail Antivirus** - If checked, scans incoming and outgoing messages for the presence of malicious objects. It is launched when the operating system loads, is located in computer RAM and scans all email messages received via the POP3, SMTP, IMAP, MAPI and NNTP protocols.

Security Level

- **Security Level**
 - **High** - Set this level if you suspect a computer has a high chance of being infected.
 - **Recommended** - This level provides an optimum balance between the efficiency and security and is suitable for most cases.
 - **Low** - If machine operates in a protected environment low security level may be suitable. A low security level can also be set if the machine operates with resource-consuming applications.
 - **Custom** - When any other setting on this tab is changed, the **Security Level** is set to **Custom**. Reset the **Security Level** to High, Recommended or Low to reset options to their default settings.

Action on Threat Detection

- **Select action automatically** - If checked, automatically performs actions recommended by Kaspersky Lab. Once a threat is detected, the application attempts to disinfect the object. If disinfect fails, the application attempts to delete it. Suspicious objects are skipped without processing. If blank, protection uses the customized settings below.
- **Select Action**
 - **Disinfect** - If checked, an attempt is made to disinfect a quarantined file.
 - **Delete if disinfection fails** - If a quarantine file fails to be disinfect, it is deleted.
 - If both of the above are unchecked, the file is skipped, and the threat is added to the **Detections** page.

Protection Scope

- **Check incoming messages only** - If checked, only incoming email is scanned. If blank, both incoming and outgoing email is scanned.

Connectivity

- **POP3/SMTP/NMTP/IMAP Traffic** - If checked, scans POP3/SMTP/NMTP/IMAP email traffic.
- **Additional: Microsoft Office Outlook Plug-in** - If checked, installs a plugin for the Outlook email client that enables the configuration of email antivirus options using the **Tools > Options > Mail Anti-Virus tab** in Outlook.
- **Additional: The Bat! Plug-in** - If checked, installs a plugin for The Bat! email client that enables the configuration of email antivirus options using the **Properties > Settings > Virus protection** item in The Bat!

Scan of Compound Files

- **Scan Attached Archives** - If checked, scans archived files.
- **Do Not Scan Archives Larger Than X MB** - Specifies the maximum size of archive to scan.
- **Do Not Scan Archives For More Than X Seconds** - Specifies the maximum time to scan archives.

Scan Methods

- **Heuristics Analysis** - If checked, uses heuristics analysis to identify the behavior of objects as malicious or suspicious, even if they are not yet identified as known threats in the signature database. This allows new threats to be detected even before they have been researched by virus analysts.
- **Depth** - Depth of heuristic analysis to use: Light, Medium, Deep.

Web Antivirus tab

Antivirus > Configuration > Profiles > New or Edit > Protection > Web Antivirus

If enabled, **Web Antivirus** scans traffic that arrives on the user's computer via the HTTP and FTP protocols, and checks whether URLs are listed as malicious or phishing web addresses.

- **Enable Web Antivirus** - If checked, ensures security while using the Internet. It protects your computer against data coming into your computer via the HTTP protocol, and also prevents dangerous scripts from being executed on the computer.

Security Level

- *Security Level*
 - **High** - Set this level if you suspect a computer has a high chance of being infected.
 - **Recommended** - This level provides an optimum balance between the efficiency and security and is suitable for most cases.
 - **Low** - If machine operates in a protected environment low security level may be suitable. A low security level can also be set if the machine operates with resource-consuming applications.
 - **Custom** - When any other setting on this tab is changed, the **Security Level** is set to **Custom**. Reset the **Security Level** to **High**, **Recommended** or **Low** to reset options to their default settings.

Action on Threat Detection

- **Select action automatically** - If checked, automatically performs actions recommended by Kaspersky Lab. Once a threat is detected, the application attempts to disinfect the object. If disinfect fails, the application attempts to delete it. Suspicious objects are skipped without processing. If blank, protection uses the customized settings below.
- *Select Action*
 - **Allow Download**
 - **Block Download**

Scan Methods

- **Check if links are listed in the database of malicious URLs** - If checked, scans the links of email messages included in the database of suspicious web addresses.
- **Heuristics Analysis for detecting viruses** - If checked, uses heuristics analysis to identify the behavior of objects as malicious or suspicious, even if they are not yet identified as known threats in the signature database. This allows new threats to be detected even before they have been researched by virus analysts.
- **Depth** - Depth of heuristic analysis to use: **Light**, **Medium**, **Deep**.

Anti-Phishing Settings



- **Check if links are listed in the database of phishing URLs** - If checked, scans the links of email messages included in the database of phishing web addresses.
- **Heuristics Analysis for detecting phishing links** - If checked, uses heuristics analysis to identify the behavior of objects as malicious or suspicious, even if they are not yet identified as known threats in the signature database. This allows new threats to be detected even before they have been researched by virus analysts.

Actions

- **Limit web traffic caching time** - If checked, limits the time allowed to scan each fragment of an object separately as it is downloaded. If the limit is exceeded for a fragment, the fragment is downloaded without scanning. If blank, fragment scanning is never skipped. In either case, the entire object is scanned once it is completely downloaded. Useful when you want to speed up scanning.

IM Antivirus tab

Antivirus > Configuration > Profiles > New or Edit > Protection > IM Antivirus

If enabled, **IM Antivirus** scans traffic that arrives on the computer via instant messaging protocols. It ensures the safe operation of numerous instant messaging applications.

- **Enable IM Antivirus** - If checked, ensures safe operation of IM clients. It protects the information that comes to your computer via IM protocols. The product ensures safe operation of various applications for instant messaging, including ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent and IRC.

Protection Scope

- **Check incoming messages only** - If blank, both incoming and outgoing messages are scanned.

Scan Methods

- **Check if links are listed in the database of malicious URLs** - If checked, scans the links of email messages included in the database of suspicious web addresses.
- **Check if links are listed in the database of phishing URLs** - If checked, scans the links of email messages included in the database of phishing web addresses.

Network Attack Blocker tab

Antivirus > Configuration > Profiles > New or Edit > Protection > Network Attack Blocker

If enabled, **Network Attack Blocker** inspects inbound network traffic for activity that is typical of network attacks. On detecting an attempted network attack that targets your computer, network activity is blocked from the attacking computer. (R)

- *Enable Network Attack Blocker*
- **Add the attacking computer to the list of blocked computers for X Minutes**

Exclusions

- **Addresses of exclusions comma delimited** - Specifies IP addresses to be excluded. Accepts both IPv4 and IPv6 CIDR address notation. Example: 1.2.3.4/24,1234::cdef/96.
 - If no slash character is included with an IPv4 address, such as 1.2.3.4, then /32 is appended.
 - If no slash character is included with an IPv6 address, such as 1234::cdef, then /128 is appended.

System Watcher tab

Antivirus > Configuration > Profiles > New or Edit > Protection > System Watcher

If enabled, **System Watcher** records application activity on the computer and provides this information to other components to ensure more effective protection.

- *Enable System Watcher*
- **Enable Exploit Prevention**
- **Do not monitor the activity of applications that have a digital signature**
- **Roll back malware actions during disinfection**
- **On detecting malware activity** - If application activity matches a behavior stream signature, the following action is performed:
 - **Select Action Automatically**
 - **Move File to Quarantine**
 - **Terminate the Malicious Program**
 - **Skip**

Scheduled Tasks tab

Critical Scan tab

Antivirus > Configuration > Profiles > New or Edit > Schedule Tasks > Critical Scan

A **Critical Scan** scans operating system startup objects.

Security Level

- **Security Level** - Three security levels are provided:
 - **High** - Set this level if you suspect a computer has a high chance of being infected.
 - **Recommended** - This level provides an optimum balance between the efficiency and security and is suitable for most cases.
 - **Low** - If machine operates in a protected environment low security level may be suitable. A low security level can also be set if the machine operates with resource-consuming applications.

Action on Threat Detection

- **Select action automatically** - If checked, automatically performs actions recommended by Kaspersky Lab. Once a threat is detected, the application attempts to disinfect the object. If disinfect fails, the application attempts to delete it. Suspicious objects are skipped without processing. Pop-up messages inform the user about new events. If blank, protection uses the customized settings below.

- **Select Action**
 - **Disinfect** - If checked, an attempt is made to disinfect a quarantined file.
 - **Delete if disinfection fails** - If a quarantine file fails to be disinfected, it is deleted.

Schedule

- **Type**
 - **Manually** - Updates of machines using this profile are only scheduled manually. Update machines manually using the control panel of the **Machines** page.
 - **By schedule** - Schedules scans of machines using this profile by the specified number of time periods. Time is agent-based.

The following field display if By Schedule is selected.

- **Time Frame** - **Hourly**, **Daily**, **Weekly**, **Monthly**
 - If **Hourly** is selected, **Run Every X Hours** displays.
 - If **Daily** is selected, **Run Every X Days** displays.
 - If **Weekly** is selected, **Sunday through Saturday** displays.
 - If **Monthly** is selected, **Run Every X Months** displays.
- **Scan Run Time (agent time)** - Displays only if Daily, Weekly or Monthly is scheduled.
- **Postpone running after application startup for X minutes**
- **Run skipped tasks** - Displays only if Daily, Weekly or Monthly is scheduled. If checked and the machine is offline when the task is scheduled to be run, run this task as soon as the machine re-connects. If unchecked and the machine is offline, skip and run the next scheduled period and time.
- **Suspend scheduled scans when screensaver is off or computer is unlocked** - If checked, scanning is paused when the computer is being used.

FULL Scan tab

Antivirus > Configuration > Profiles > New or Edit > Schedule Tasks > Full Scan

A **Full Scan** performs a thorough **Antivirus** scan of the entire operating system, including RAM, objects that are loaded at startup, backup storage of the operating system, and all hard drives and removable drives.



Security Level

- **Security Level** - Three security levels are provided:
 - **High** - Set this level if you suspect a computer has a high chance of being infected.
 - **Recommended** - This level provides an optimum balance between the efficiency and security and is suitable for most cases.
 - **Low** - If machine operates in a protected environment low security level may be suitable. A low security level can also be set if the machine operates with resource-consuming applications.

Action on Threat Detection

Select action automatically - If checked, automatically performs actions recommended by Kaspersky Lab. Once a threat is detected, the application attempts to disinfect the object. If disinfect fails, the application attempts to delete it. Suspicious objects are skipped without processing. Pop-up messages inform the user about new events. If blank, protection uses the customized settings below.

- **Select Action**
 - **Disinfect** - If checked, an attempt is made to disinfect a quarantined file.
 - **Delete if disinfection fails** - If a quarantine file fails to be disinfected, it is deleted.

Schedule

- **Type**
 - **Manually** - Updates of machines using this profile are only scheduled manually. Update machines manually using the control panel of the **Machines** page.
 - **By schedule** - Schedules scans of machines using this profile by the specified number of time periods. Time is agent-based.

The following field display if By Schedule is selected.

- **Time Frame** - Hourly, Daily, Weekly, Monthly
 - If Hourly is selected, **Run Every X Hours** displays.
 - If Daily is selected, **Run Every X Days** displays.
 - If Weekly is selected, **Sunday through Saturday** displays.
 - If Monthly is selected, **Run Every X Months** displays.
- **Scan Run Time (agent time)** - Displays only if Daily, Weekly or Monthly is scheduled.
- **Postpone running after application startup for X minutes**
- **Run skipped tasks** - Displays only if Daily, Weekly or Monthly is scheduled. If checked and the machine is offline when the task is scheduled to be run, run this task as soon as the machine re-connects. If unchecked and the machine is offline, skip and run the next scheduled period and time.
- **Suspend scheduled scans when screensaver is off or computer is unlocked** - If checked, scanning is paused when the computer is being used.

Update tab



Antivirus > Configuration > Profiles > New or Edit > Schedule Tasks > Update

The **Update** tab schedules the downloading of **Antivirus** updates to client machines.

Schedule

- **Automatic** - Checks for updates at specified intervals. When a new update is discovered, downloads and installs them on **Antivirus** managed machines using this profile.
- **Manually** - Updates of machines using this profile are only scheduled manually. Update machines manually using the control panel of the **Machines** page.
- **By schedule** - Schedules scans of machines using this profile by the specified number of time periods. Time is agent-based.

The following field display if **By Schedule** is selected.

- **Schedule Time Frame** - **Hourly**, **Daily**, **Weekly**, **Monthly**
 - If **Hourly** is selected, **Run Every X Hours** displays.
 - If **Daily** is selected, **Run Every X Days** displays.
 - If **Weekly** is selected, **Sunday through Saturday** displays.
 - If **Monthly** is selected, **Run Every X Months** displays.
- **Scan Run Time (agent time)** - Displays only if Daily, Weekly or Monthly is scheduled.
- **Postpone running after application startup for X minutes**
- **Run skipped tasks** - Displays only if Daily, Weekly or Monthly is scheduled. If checked and the machine is offline when the task is scheduled to be run, run this task as soon as the machine re-connects. If unchecked and the machine is offline, skip and run the next scheduled period and time.

Additional

- **Copy Updates to Folder** - Specify the folder where updates will be copied.

Custom Scan tab

Antivirus > Configuration > Profiles > New or Edit > Schedule Tasks > Custom Scan

A **Custom Scan** scans unprocessed files. An infected file is considered *unprocessed* if no action —such as disinfect, delete, or block—was taken while scanning the computer for viruses and other threats. An infected file may be unprocessed, for example, because it is located on a drive without write privileges, or action on the file was intentionally skipped after notifying the user.



Security Level

- **Security Level**
 - **High** - Set this level if you suspect a computer has a high chance of being infected.
 - **Recommended** - This level provides an optimum balance between the efficiency and security and is suitable for most cases.

- **Low** - If machine operates in a protected environment low security level may be suitable. A low security level can also be set if the machine operates with resource-consuming applications.
- **Custom** - When any other setting on this tab is changed, the **Security Level** is set to **Custom**. Reset the **Security Level** to **High**, **Recommended** or **Low** to reset options to their default settings.

Action on Threat Detection

- **Select action automatically** - If checked, automatically performs actions recommended by Kaspersky Lab. Once a threat is detected, the application attempts to disinfect the object. If disinfect fails, the application attempts to delete it. Suspicious objects are skipped without processing. If blank, protection uses the customized settings below.
- **Select Action**
 - **Disinfect** - If checked, an attempt is made to disinfect a quarantined file.
 - **Delete if disinfection fails** - If a quarantine file fails to be disinfected, it is deleted.
 - If both of the above are unchecked, the file is skipped, and the threat is added to the **Detections** page.

Schedule

- **Type**
 - **Manually** - Updates of machines using this profile are only scheduled manually. Update machines manually using the control panel of the **Machines** page.
 - **By schedule** - Schedules scans of machines using this profile by the specified number of time periods. Time is agent-based.

The following field display if By Schedule is selected.

- **Time Frame** - **Hourly**, **Daily**, **Weekly**, **Monthly**
 - If **Hourly** is selected, **Run Every X Hours** displays.
 - If **Daily** is selected, **Run Every X Days** displays.
 - If **Weekly** is selected, **Sunday through Saturday** displays.
 - If **Monthly** is selected, **Run Every X Months** displays.
- **Scan Run Time (agent time)** - Displays only if Daily, Weekly or Monthly is scheduled.
- **Postpone running after application startup for X minutes**
- **Run skipped tasks** - Displays only if Daily, Weekly or Monthly is scheduled. If checked and the machine is offline when the task is scheduled to be run, run this task as soon as the machine re-connects. If unchecked and the machine is offline, skip and run the next scheduled period and time.
- **Suspend scheduled scans when screensaver is off or computer is unlocked** - If checked, scanning is paused when the computer is being used.

Vulnerability Scan tab

Antivirus > Configuration > Profiles > New or Edit > Schedule Tasks > Vulnerability Scan

A **Vulnerability Scan** looks for errors in programming or design, weak passwords, malware activity, anomalies, damaged and settings.

Schedule

- **Type**
 - **Manually** - Updates of machines using this profile are only scheduled manually. Update machines manually using the control panel of the **Machines** page.
 - **By schedule** - Schedules scans of machines using this profile by the specified number of time periods. Time is agent-based.

The following field display if By Schedule is selected.

- **Time Frame** - **Hourly**, **Daily**, **Weekly**, **Monthly**
 - If **Hourly** is selected, **Run Every X Hours** displays.
 - If **Daily** is selected, **Run Every X Days** displays.
 - If **Weekly** is selected, **Sunday through Saturday** displays.
 - If **Monthly** is selected, **Run Every X Months** displays.
- **Scan Run Time (agent time)** - Displays only if Daily, Weekly or Monthly is scheduled.
- **Postpone running after application startup for X minutes**
- **Run skipped tasks** - Displays only if Daily, Weekly or Monthly is scheduled. If checked and the machine is offline when the task is scheduled to be run, run this task as soon as the machine re-connects. If unchecked and the machine is offline, skip and run the next scheduled period and time.

Exclusions tab

Antivirus > Configuration > Profiles > New or Edit > Exclusions

An exclusion is a combination of conditions set in Trusted zone that allows Kaspersky Endpoint Security for Windows skip a particular object during an antivirus scan.

The **Exclusions** tab for **Antivirus** profiles excludes objects from **Antivirus** monitoring.



- **Include Global Settings** - If checked, **Global Exclusions** are enabled for this profile.

Exclusion Rules

- **New** - Adds file masks or directory path masks to be excluded from scanning and protection, up to a limit of 256 exclusions.

- **Delete** - Deletes a selected exclusion rule. Supported exclusions include:

- Masks without file paths
 - *.exe — all files with the EXE extension.
 - *.ex? - all files with the EX? extension, where ? can represent any single character.
 - test - all files named test.
- Masks with absolute file paths
 - C:\dir*.* or C:\dir* or c:\dir\ - all files in the C:\dir\ folder.
 - C:\dir*.exe - all files with the exe extension in the C:\dir\ folder.
 - C:\dir*.ex? - all files with the ex? extension in folder C:\dir\ folder, where ? can represent any single character.
 - C:\dir\test - only the C:\dir\test file.
 - C:\dir\dir*\file.exe — the file.exe file located in the C:\dir\dir* folder, where * stands for any number of characters.
 - C:\dir\dir???\file.exe — the file.exe file located in the C:\dir\dir??? folder, where ? stands for one character.
- File path masks
 - dir*.*, or dir* - all files in all dir\ folders.
 - dir\test - all test files in dir\ folders.
 - dir*.exe - all files with the exe extension in all dir\ folders.
 - dir*.ex? - all files with the ex? extension in all dir\ folders, where ? can represent any

Trusted Apps

Trusted applications are not monitored for suspicious activity, file activity, network activity and attempts to access the system registry.

- **New** - Add the full path and filename of an executable.
- **Delete** - Deletes a selected application path and filename.

Use standard environment variable notation to specify the location of applications. Examples:

- %SystemRoot%\system32\svchost.exe
- %ProgramFiles%\Messenger\msmsgs.exe
- %ProgramFiles%\MSN Messenger\MsnMsgr.Exe



Trusted URLs

Trusted URLs are not monitored for viruses by **Web Antivirus**

- **New** - Adds a URL.
- **Delete** -

Deletes a

selected URL.

Formatting

guidelines:

- Enter **http://** or **https://** before any address.
- * - Use to represent any combination of characters. Example: **http://www.CloudActiv8.com/***
- ? - Use to represent any one character. Example: **http://Patch_123?.com**
- If an * or ? is part of an actual URL, when you add the URL to the Trusted URL list, you must use a backslash to override the * or ? following it. Example: **http://www.CloudActiv8.com/test\?**

Advanced Settings tab

Antivirus > Configuration > Profiles > New or Edit > Advanced Settings

- **Enable Self-Defense** - Prevents unauthorized access to **Antivirus** files, including protection against auto-clickers.
- *Disable external management of the system service*
- **Enable dump writing**
- **Send dump and trace files to Kaspersky Lab for analysis**

Operating Mode

- **Do not start scheduled tasks while running on battery power**
- **Concede Resources To Other Applications** - If checked, when the load on the file system from other applications increases, scan tasks will pause their activity.



Proxy Settings

- **Use proxy server** - If checked, manually specify the proxy server used to download updates. If blank, proxy settings are automatically detected.
 - **Address** - Enter a valid proxy server name or IP address.
 - **Port** - Enter a port number.
- **Specify Authentication Data** - If checked, proxy authentication is required.
 - *User Name*
 - **Password**

- **Bypass proxy server for local addresses** - If checked, local IP addresses do not use the proxy server.

Scan Removable Drivers onConnection

- **Scan Removable Drivers** - Do Not Scan, Detailed Scan, Quick Scan.

Install Procedures

- *Pre Procedure*
- **Post-Procedure**

Uninstall Procedures

- **Pre Procedure**
- **Post-Procedure**

Reboot Options

Antivirus > Configuration > Profiles > New or Edit > Reboot Options

Reboot prompts and warnings occur after the update.

- *When the user is logged in*
- Reboot after update
- Warn user and wait for x min and then reboot
- Ask user about reboot and offer to delay (reask every x minute); do not reboot until get response
- Ask permission, if no response in x min reboot
- Skip Reboot
- Do not reboot after update, send email
- **Wait time** - Minutes to wait after warning the user of reboot.
- *When a user is not logged in*
- Reboot after update
- Skip Reboot
- Do not reboot after update, send email

Endpoints tab

Antivirus > Configuration > Profiles > Endpoints

The **Endpoints** tab lists all machines using the selected **Antivirus** profile.

Alerts

Antivirus > Configuration > Alerts

The **Alerts** page manages **Antivirus** alert profiles. Each alert profile represents a different set of alert conditions and actions taken in response to an alert. Multiple alert profiles can be assigned to the same endpoint. Changes to an alert profile affect all machine IDs assigned that alert profile. An alert profile is assigned to machine IDs using **Antivirus > Machines > Alert Profiles**. Different types of machines may require different alert profiles. Alert profiles are visible to all CloudActiv8 users.

Reviewing Alarms Created by Antivirus Alerts

- Monitor > **Alarm Summary**
- Monitor > Dashboard List > any **Alarm Summary Window** within a dashlet
- Agent > Agent Logs > **Agent Log**
- The Agent > Agent Logs > **Monitor Action Log** - Shows the actions taken in response to an alert, whether or not an alarm was created.
- **Live Connect** > Asset > Log Viewer > Alarm
- Info Center > Reporting > Legacy Reports > Logs > Alarm Log

Actions

- **New** - Creates a new alert profile.
- **Edit** - Edits an existing alert profile. You can also double-click an alert profile to open it.
- **Delete** - Deletes an existing alert profile.
- **Copy** - Saves a selected alert profile with new name.
- **Alerts Configuration** - Configures the format of each type of alert notification message.

Table Columns

- **Name** - Name of the alert profile.
- **Description** - A description of the alert profile.

Summary tab

Antivirus > Configuration > Alerts > New or Edit > Summary tab

General

- **Name** - The name of the alert profile.
- **Description** - A description of the alert profile.

De-duplication

- **Filter duplicate alerts** - Prevents duplicate alerts from being generated for a specified number of time periods.
 - **Time Frame** - Days
 - **Every X days** - Number of time periods to suppress duplicate alerts.

Alert Types tab

Antivirus > Configuration > Alerts > New or Edit > Alert Types tab

The **Alerts Types** tab specifies the conditions that cause an **Antivirus** or **Anti-Malware** alert to be created. The format for notifying users about each alert type can be changed using the **Alerts Configuration** button.

Select Alerts Types



- **Security application removed by user** - A managed security product was uninstalled from the endpoint.
- **Protection disabled (entire engine)** - A managed security product's protection has been disabled.
- **Definition not updated in X days / Number of days** - A managed security product's definitions have not been updated in a specified number of days.
- **Definition update did not complete** - The update of a managed security product's definitions was not completed.
- **Active threat detected** - An active threat has been detected. An active threat is a detection that has not been healed or deleted. User intervention is required using the **Detections** page.

- **Threat detected and healed** - A threat was detected and healed. No user intervention is required.
- **Scan did not complete** - A scan did not complete.
- **Reboot required** - A reboot is required.
- **Profile not compliant** - An endpoint is not compliant with its profile.
- **Profile assignment failed** - The assignment of a profile to a machine failed.
- **Client install failed** - A managed security product install failed.
- **Client repair failed** - A managed security product repair failed.
- **Client uninstall failed** - A managed security product uninstall failed.
- **Client license deactivated** - A managed security product license was deactivated.

Actions tab

Antivirus > Configuration > Alerts > New or Edit > Actions tab

The **Actions** tab of an alert profile determines the actions taken in response to any of the **Alert Types** encountered by an endpoint assigned that alert profile.

- **Create Alarm** - If checked and an alert type is encountered, an alarm is created.
- **Create Ticket** - If checked and an alert condition is encountered, a ticket is created.
- **Email Recipients (comma separated)** - If checked and an alert condition is encountered, an email is sent to the specified email addresses.
- **Script Name to Run** - If an alert condition is encountered, run the selected agent procedure.
- **Users Notified in Info Center** - If checked and an alert condition is encountered, a notification is sent to the specified user's Info Center > **Inbox**
- **Send Message to Notification Bar** - If checked and an alert condition is encountered, a notification is sent to the specified user's **Notification Bar**

Endpoints tab

Antivirus > Configuration > Alerts > New or Edit > Endpoints

The **Endpoints** tab lists all machines using the selected alerts profile.

Actions



- **Add** - Add a new machine
- **Delete** - Deletes selected machine from the list of machines below.

Settings

Antivirus > Configuration > Settings

The **Settings** page maintains module-level preferences.

Global Exclusions tab

Antivirus > Configuration > Settings > Global Exclusions

The **Global Exclusions** tab excludes objects from **Antivirus** monitoring. You can optionally apply these global exclusions by checking the **Include Global Settings** checkbox on the **Exclusions** tab of the profile.

All CloudActiv8-related folders and CloudActiv8 agent-related applications are added to **Global Exclusions** by default.

Exclusion Rules

- **New** - Adds file masks or directory path masks to be excluded from scanning and protection, up to a limit of 256 exclusions.
- **Edit** - Edits the selected exclusion rule.
- **Delete** - Deletes a

selected exclusion rule.

Supported exclusions include:

Masks without file paths

- ***test*** - any file with **test** in name, saying 12astestsdsd.sds
- ***test.*** - any file with name ending on test: 346dfghtest.gdh
- **test.*** - file with name **test** and any extension
- Masks with absolute file paths
 - **C:\dir*.*** or **C:\dir*** or **c:\dir** - all files in the **C:\dir** folder
 - **C:\dir*.exe** - all files with the **exe** extension in the **C:\dir** folder
 - **C:\dir*.ex?** - all files with the **ex?** extension in folder **C:\dir**, where **?** can represent any single character
 - **C:\dir\test** - only the **C:\dir\test** file
- File path masks
 - **dir*.***, or **dir*** - all files in all **dir** folders
 - **dir\test** - all test files in **dir** folders
 - **dir*.exe** - all files with the **exe** extension in all **dir** folders
 - **dir*.ex?** - all files with the **ex?** extension in all **dir** folders, where **?** can represent any single character

Trusted Apps

Trusted applications are not monitored for suspicious activity, file activity, network activity and attempts to access the system registry.

- **New** - Add the full path and filename of an executable.
- **Edit** - Edits the selected application path and filename.
- **Delete** - Deletes a selected application path and filename.

Use standard environment variable notation to specify the location of applications. Examples:

- %SystemRoot%\system32\svchost.exe
- %ProgramFiles%\Messenger\msmsgs.exe
- %ProgramFiles%\MSN Messenger\MsnMsgr.Exe

Trusted URLs

Trusted URLs are not monitored for viruses by **Web Antivirus**

- **New** - Adds a URL.
- **Edit** - Edits the selected URL.
- **Delete** -

Deletes a selected URL.

Formatting

guidelines:

- Enter **http://** or **https://** before any address.
- * - Use to represent any combination of characters. Example: <http://www.CloudActiv8.com/>*
- ? - Use to represent any one character. Example: http://Patch_123?.com
- If an * or ? is part of an actual URL, when you add the URL to the Trusted URL list, you must use a backslash to override the * or ? following it. Example: <http://www.CloudActiv8.com/test\?>

Application Settings tab

Antivirus > Configuration > Settings > Application Settings

The **Application Settings** tab sets options that apply to the entire module.



Actions

- **Edit** - Edits general settings
- Private Profiles** - If checked, profiles are only visible if the profile was created by you or if the profile is assigned to a machine assigned to the scope you are using. Profiles are public by default.

- **Use LAN Updater** - If checked, enables peer-to-peer file downloading of Kaspersky definition files using **LAN Cache**. Before enabling this feature you must:
 - ✓ Designate an Antivirus-installed machine as a LAN Cache machine using the Agent > **LAN Cache** page.
 - ✓ Assign that LAN Cache to other Antivirus-installed machines on the same network, using the Agent > **Assign LAN Cache** page.
- **Refresh Lan Updater** - Once **Use LAN Updater** is checked, click **Use LAN Update** to enable this feature on newly added or reconfigured machines. As a precaution, the **Refresh Lan Updater** function runs once a day.

Licensing Alerts tab

Anti-Malware > Configuration > Settings > Licensing Alerts

The **Licensing Alerts** tab specifies the conditions that cause an **Antivirus** or **Anti-Malware** licensing alert to be created. It also specifies the actions taken in response to any of the alert types.

Actions

- **Edit** - Edits licensing alert.

Alert Types

- **Available licenses less than X** - The number of available license is less than a specified number.
- **License expiring in X days** - The license is expiring in a specified number of days.
- **License expired and not renewed** - An expired license has not been renewed.

Actions tab

- **Email Recipients (comma separated)** - If checked and an alert condition is encountered, an email is sent to the specified email addresses.
- **Users Notified in Info Center** - If checked and an alert condition is encountered, a notification is sent to the specified user's Info Center > **Inbox**
- **Send Message to Notification Bar** - If checked and an alert condition is encountered, a notification is sent to the specified user's **Notification Bar**

Administration

Application Logging

Antivirus Application Logging

The **Application Logging** page displays a log of **Antivirus** module activity by:

- **Event ID**
- **Event Name**
- **Message**
- **Admin**
- **Event Date**

This table supports selectable columns, column sorting, column filtering and flexible columns widths.

