Antivirus

User Guide

Version R91

English

July 15, 2015

Agreement

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

Contents

Antivirus Overview 1
Antivirus Module Requirements 3
Machines 3
- Page Layout 4
- Explorer Grid 4
- Control Panel 6
- Antivirus Columns 9
- Details Panel 10
- Antivirus Agent Menu 12

Dashboards 12
Detections 13
Profiles 14
- Summary tab 15
- Protection tab 16
- Quick Scan / Critical Scan tab 19
- Full Scan tab 20
- Update Options tab 21
- Exclusions tab 21
- Endpoints tab 23

Alerts 23
- Summary tab 24
- Alert Types tab 24
- Actions tab 24
- Endpoints tab 25

Index 27

Antivirus Overview

Antivirus (KAV) 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 **AntiMalware**.

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.
- Upgrade Ready option to help you identify and upgrade out-of-date **Antivirus** clients.
- Policy Management can manage the assignment of **Antivirus** profiles.
- Specialized agent procedures are provided with **Antivirus** that enable you to "pre-deploy" the **Antivirus** installer package to endpoints, reducing required bandwidth. See the **knowledge base article** *(https://helpdesk.kaseya.com/entries/34261116)*.
- **Customize the user interface of the Antivirus client on the endpoint** *(https://helpdesk.kaseya.com/entries/32410117)*.

> **Note:** **Antivirus** 6.5 supports both Kaspersky version 10 and legacy version 6, for workstation and server endpoints. Specialized profiles are provided to manage each type of machine. *Kasperksy version 2010 endpoints are not supported in* **Antivirus** *6.5.* **Antivirus** 6.5 only installs or upgrades endpoints to Kaspersky version 10. *Version 10 is strongly recommended.* You can upgrade a Kaspersky version 6 endpoint to Kaspersky version 10 using the Install > **Upgrade Client Version** button on the Control Panel.

LAN Cache

LAN Cache enables multiple machines to retrieve the same files from a local LAN machine instead of repeatedly downloading them from the Kaseya Server. This reduces network bandwidth issues. Files downloaded for **Antivirus** endpoints—install packages, updates and antivirus definitions—use LAN Cache automatically, if LAN Cache is already configured for those endpoints. No additional configuration in **Antivirus** is required. See Agent > **LAN Cache** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#9328.htm)* for more information.

> **Note:** See **Antivirus System Requirements** *(page 3)*.

Functions	Description
Machines *(page 3)*	Installs and uninstalls Antivirus software on selected

	machines and provides a detailed view of the Antivirus status of any selected machine.
Dashboards *(page 12)*	Displays a dashboard view of the status of all machines installed with Antivirus.
Detections *(page 13)*	Displays virus threats you can take action on.
Profiles *(page 14)*	Manages Antivirus profiles that are assigned to machine IDs.
Alerts *(page 23)*	Manages Antivirus module alerts.

Antivirus Module Requirements

Kaseya Server

- The Antivirus R91 module requires VSA R91

Agent Requirements

- KAV R91 requires agent version 8.0.0.0 or higher.

Requirements for Each Managed Workstation

- 1 GHz CPU or greater
- 1 GB available RAM
- 1 GB free space on the hard drive
- Microsoft Windows XP SP3, Vista, 7, 8, 8.1 are supported.
- Microsoft Windows Installer 3.0
- See **Kaspersky Anti-Virus for Windows Workstation version 10.x** *(http://support.kaspersky.com/kes10wks#requirements)* for a complete list of workstation system requirements.

Requirements for Each Managed Server

- Server 2003, 2003 R2, SBS 2003 R2, 2008 SP1, SBS 2008 SP1, 2008 R2 SP1, SBS 2011, 2012, 2012 R2 are supported.
- Only the OS of SBS 2011 is supported. It does not include Exchange email servers hosted by SBS 2011.
- See **Kaspersky Anti-Virus for Windows Servers version 10.x** *(http://support.kaspersky.com/kes10fs#requirements)* for a complete list of server system requirements, *including service pack requirements for each OS*.

> **Note:** See general **System Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9010000/reqs/index.asp#home.htm)*.

Machines

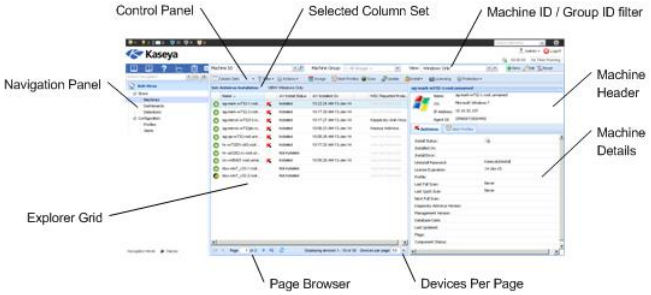
Antivirus > Show > Machines

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** *(page 4)*
- **Explorer Grid** *(page 4)*
- **Control Panel** *(page 6)*
- **Antivirus Columns** *(page 9)*
- **Detail Panel** *(page 10)*
- **Antivirus Agent Menu** *(page 12)*

Page Layout

The layout of the **Machines** *(page 3)* page comprises the following design elements:



- **Navigation Panel** - Used to navigate to pages within the **Antivirus** module.
- **Explorer Grid** - Each managed machine in the VSA 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.

Explorer Grid

The **Explorer Grid** of the **Machines** *(page 3)* page lists each machine currently installed with **Antivirus** *and* included in the **machine ID / group ID filter** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#209.htm)*.

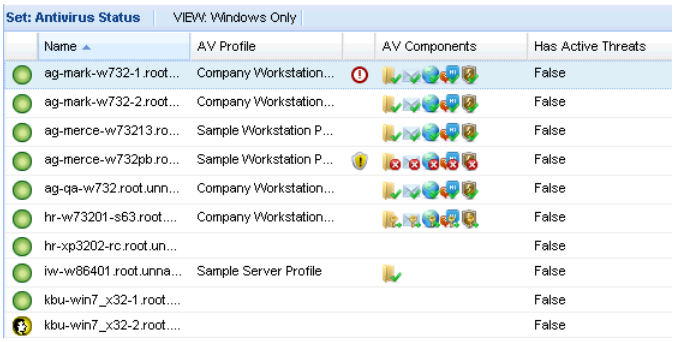
Note: The only exception is when the `Antivirus Installation` is selected. In this case all machines included the machine ID /group ID filter are displayed.

- The *set of columns* displayed is determined by the **Column Set** selection in the **Control Panel** *(page 6)*. The currently selected column set displays in the bar just above the **Explorer Grid**.

  Note: See ***Antivirus Columns*** *(page 9)* for a description of each column available to display in *any* **Explorer Grid** column set.

- Page forward displays multiple pages of machines.

- Machines per page sets the number of rows on each page.



Column Icons

	definitions out of date
	reboot required
	full scan in progress
	license expired
	endpoint configuration out of compliance with the profile
	pending assign
	pending enable
	pending disable
	scan pending
	uninstall pending
	verify pending
	install pending
	update pending
	install failed
	install successful
	Endpoint Security is installed on this machine

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 3)* page executes tasks, either for the entire **Explorer Grid** *(page 4)* or for a single selected machine.

Column Sets

Selecting a column set displays a predefined set of columns.

- **Modify Columns** - Customizes the set of columns displayed by *any* column set.

  Note: See **Antivirus Columns** *(page 9)* for a description of each column available to display in *any* **Explorer Grid** column set.

- **Antivirus Installation** - Displays **Antivirus** installation columns in the **Explorer Grid** *for all agent machines*.
- **Antivirus Status** - Displays status columns in the **Explorer Grid** for all agent machines *installed with an* **Antivirus** *client.*

Filter

Filters the list of rows displayed by software installed, upgrade recommended, reboot required, definitions out of date, machine out of compliance with profile, latest version installed, or unsupported clients.

Note: The `Antivirus Upgrade Recommended` filter helps you identify which machines are eligible for upgrading to the latest version. To upgrade, install over an existing installation of **Antivirus**.

Actions

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

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** *(page 14)* for more information.

Alert Profiles

Assigns or removes an alert profile for selected machines. The **Alert Profiles** tab on the **Details Panel** *(page 10)* displays all profiles assigned to a machine.

Scan

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

- **Start Date** - The start date of the scan.

- **Time** - The start time of the scan.
- **Distribution Window** - Reschedules multiple scans evenly across a distribution window no later than the number of periods specified, to spread network traffic and server loading.

For **Antivirus** there are two types of scan:

- **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.
- **Quick / Critical Area Scan** - Virus scan of operating system startup objects. Quick Scan was renamed to Critical Scan starting with **Antivirus** version 10.x

Update

Schedules an update on selected machines with the latest **Antivirus** definitions.

- **Start Date** - The start date of the update.
- **Time** - The start time of the update.
- **Distribution Window** - Reschedules multiple updates evenly across a distribution window no later than the number of periods specified, to spread network traffic and server loading.

Install

- **Install or Upgrade Antivirus** - Installs or upgrades the **Antivirus** client on selected machines.

> **Warning:** Kaseya does not support installing agents in the `%windir%` (typically `c:\windows`) directory.

  - **Profile Selection** - 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 profle. Only version 10.x workstation and server profiles can be selected.
  - **Allow Reboot** - If checked, allows a reboot if necessary. For workstations only, a reboot is required after an install.
  - **Advanced Options** - Click to display the following options.
    - ✓ **Start Date & Time** - The start date and start time of the install.
    - ✓ **Distribution Window** - Reschedules multiple installs evenly across a distribution window no later than the number of periods specified, to spread network traffic and server loading.
    - ✓ **Prompt before install** - If checked, the Installation only proceeds if the user is logged on and agrees to proceed.
    - ✓ **Skip if Offline** - If checked, skips the install if the computer is offline at the time the install is scheduled to run. If blank, the installation occurs when the computer comes back online.
    - ✓ **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 password displays in the **Details Panel** *(page 10)*. Passwords must be alphanumeric. Special characters are not supported.

> **Warning:** The password can only be set during the initial install. You must uninstall the endpoint to change an existing password.

    - ✓ **Blocking Install Issues** - Lists issues that can prevent a successful installation on selected machines.

> **Note:** Specialized agent procedures are provided with **Antivirus** that enable you to "pre-deploy" the **Antivirus** installer package to endpoints, reducing required bandwidth. See the **knowledge base article** *(https://helpdesk.kaseya.com/entries/34261116)*.

- **Uninstall Antivirus** - Uninstalls the **Antivirus** client on selected machines.
  - **Start Date** - The start date of the uninstall.
  - **Time** - The start time of the uninstall.
  - **Distribution Window** - Reschedules multiple uninstalls evenly across a distribution window no later than the number of periods specified, to spread network traffic and server loading.
- **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 VSA.
  - **Start Date** - The start date of the repair.
  - **Time** - The start time of the repair.
  - **Distribution Window** - Reschedules multiple repairs evenly across a distribution window no later than the number of periods specified, to spread network traffic and server loading.
- **Connect Kaseya Antivirus** - Re-establishes a connection to a machine that was previously managed by **Antivirus** but had the Kaseya agent removed, then re-installed. This includes re-establishing a connection to machines that were managed by a different VSA.
  - **Start Date** - The start date of the repair.
  - **Time** - The start time of the repair.
  - **Distribution Window** - Reschedules evenly across a distribution window no later than the number of periods specified, to spread network traffic and server loading.
  - **Profile Selection** - Selects the workstation profiles and server profiles that are applied.

Licensing

> **Note:** As of version 9.1 licensing sets the expiration date of the license to one year from the day it is purchased, irrespective of the day it is installed. The expiration dates of existing licenses are not affected by this change.

- **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** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#2924.htm)* page.
  - Total Purchased to date
  - Full Available (Purchased not allocated, applied, partial or expired)
  - Allocated (Scheduled for install, but install not yet complete)
  - Applied (Active license applied to a machine)
  - Partial Available (Formerly assigned to a machine but returned to pool before expiration)
  - Partial Allocated (Partial Available that has been scheduled for install, but install not yet complete)
  - Total (purchase licenses minus expired)
  - Expired Licenses
  - No of Days Remaining - Days remaining before all Antivirus licenses expire. For service providers with permanent licenses the license expiration date is December 31, 2032.

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.

Antivirus Columns

Column sets determine the columns displayed in the **Explorer Grid** *(page 4)*. You can edit *any* column set listed in the **Column Set** drop-down list of the **Control Panel** *(page 6)*.

1. Select a column set from the **Column Set** drop-down list.
2. Select **Modify Columns** in the same drop-down list to display the **Edit Column Set** window.

   The assigned columns in the right-hand list are the columns that will be displayed when you save your changes to the column set.

The following columns are available to select when modifying *any* column set in the **Explorer Grid** *(page 4)*. Select **Column Set** in the **Control Panel** *(page 6)* to modify a column set.

Antivirus

- **AV Expiration Date** - The date **Antivirus** security is scheduled to expire.
- **AV Install Status** - `Not Installed`, `Script Scheduled`, `Installed`
- **Install Phase Icon** - If checked, **Antivirus** is installed on the machine.

Detections

- **Deleted** - Number of detections automatically deleted.
- **Detected** - Number of detections.
- **Disinfected** - Number of detections automatically disinfected.
- **Has Active Threats** - Number of detections that could not be automatically disinfected or deleted and require user attention.
- **Infected** - Number of detections infected.
- **Other** - Number of detections that cannot be classified under any other category. Applies when Kaspersky introduces a new detection category that **Antivirus** does not yet recognize.
- **Suspicious** - Number of suspicious detections not deleted or disinfected that a user might want to review.

Endpoint Protection

- **Agent Guid Str** - The unique GUID of the Kaseya agent, in string format.
- **Id** - The unique GUID of the Kaseya agent, in numerical format.
- **Last Reboot** - The date/time the machine was last rebooted.
- **Login Name** - The currently logged on user.
- **Name** - The machine ID.group ID.organization ID of the machine.
- **Online Status** - These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent QuickView window.
  - Online but waiting for first audit to complete
  - Agent online
  - Agent online and user currently logged on.
  - Agent online and user currently logged on, but user not active for 10 minutes
  - Agent is currently offline
  - Agent has never checked in
  - Agent is online but remote control has been disabled
  - The agent has been suspended
- **Operating System** - The operating system of the machine.
- **Time Zone Offset** - Displays the number of minutes. See System > User Settings > **Preferences** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#503.htm)*.

Scan

- **AV Next Full Scan** - The date/time the next **Antivirus** full scan is scheduled.
- **AV Last Full Scan** - The date/time the last **Antivirus** full scan was performed. An **Antivirus** full scan provides a thorough scan of the entire system. Includes: system memory, programs loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **AV Last Quick Scan** - The last date and time an **Antivirus** quick scan of operating system startup objects was performed. Quick Scan was renamed to Critical Scan starting with **Antivirus** version 10.x
- **AV Scan Status** - The status of the scan.

Security

- **AV Installed On** - The date **Antivirus** was installed.
- **AV Profile** - The **Antivirus** profile assigned to this machine.

Status

- **AV Components** - Identifies the status of **Antivirus** components installed on this machine.
- **AV Last Status Update** - (Antivirus Client Update) - The date and time the **Antivirus** client was last updated
- **AV Flags** - Possible flags include: `Definitions out of date`
- **Pending Actions** - Install, Assign, Update and Scan
- **Reboot Needed** - If `Yes`, a reboot is required.

Upgrade Ready

- **Available AV Client Version** - The Kaspersky version number of the **Antivirus** client available to upgrade on this machine.

Version

- **AV Client Version** - The Kaspersky version number of the **Antivirus** client installed on this machine.
- **AV Database Date** - (Antivirus Definition File Update) - The date and time of the **Antivirus** definition database currently being used by this machine.
- **AV Service Version** - The version of the **Antivirus** client.
- **Agent Version** - The version of the Kaseya agent.
- **Update** - The status of the update.

Windows Security Center

- **Active** - If checked, the antivirus product is being used.
- **Manufacturer** - The manufacturer of the antivirus product.
- **Up To Date** - If checked, the antivirus product is up to date.
- **Version** - The version of the antivirus product.
- **WSC Reported Product Name** - The name of the antivirus product registered with *Windows Security Center*. **Antivirus** itself does not register with *Windows Security Center*.

> **Note:** Windows 7 and later calls the *Windows Security Center* the *Action Center*.

Details Panel

Header

- **Name** - The machine ID.group ID.organization ID of the machine.

- **OS** - 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** - If checked, **Antivirus** security is installed.
- **Installed On** - The date **Antivirus** was installed.
- **Install Error** - If an install error occurs, displays a `View Log` link to the Kaspersky install log.
- **Uninstall Password** - The password required to reconfigure or uninstall the **Antivirus** 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 Quick Scan** - The last date and time a critical area scan of operating system startup objects was performed. Quick Scan was renamed to Critical Scan starting with **Antivirus** version 10.x
- **Next Full Scan** - The next date and time an **Antivirus** scan is scheduled to be performed.
- **Kaspersky Antivirus Version** - The Kaspersky version number of the **Antivirus** client installed on this machine.
- **Management Version** - The version number of the **Antivirus** package installed on the managed machine.
- **Antivirus Definition File Update** - The date and time of the **Antivirus** definition database currently being used by this machine.
- **Antivirus Client Update** - 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`.

  > **Note:** *Once a machine is brought back into compliance, the out of compliance flag continues to display. To clear the out of compliance flag, re-assign the profile to the machine.*

- **Component Status** - Identifies the status of **Antivirus** components installed on this machine. Component protection is specified using the Profiles > **Protection** *(page 16)* tab.

   - **Enable File Antivirus** - If checked, scans all files that are opened, saved, or executed. *Applies to workstations an servers.*

   - **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. *Applies to workstations only.*

   - **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. *Applies to workstations only.*

   - **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. *Applies to workstations only.*

   - **Enable Proactive Antivirus** - If checked, recognizes a new threat on your computer by the sequence of actions executed by a program. If, as a result of activity analysis, the sequence of application's actions arouses any suspicion, **Antivirus** blocks the activity of this application. *Applies to workstations only.*

   - **Enable Anti-Spam** - If checked, integrates with the mail client installed on your computer,

and monitors all incoming email messages for spam. All messages containing spam are marked with a special header. The component also analyzes email messages to detect phishing. *Applies to workstations only.*

- **Enable Anti-Spy** - If checked, intercepts the dialers attempting to establish a connection with pay-per-use websites and blocks them. *Applies to workstations only.*

- **Enable Access Control** - If checked, prevents the autorunning of applications and devices on removable media connected to the computer, including the running of `autorun.inf` files. *Applies to workstations only.*

Alert Profiles tab

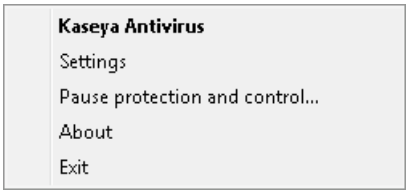
Displays the list of **alert profiles** *(page 23)* assigned to the selected machine.

Note: The Alerts > <profile> > **Endpoints** *(page 25)* tab lists all machines using a selected alerts profile.

Antivirus Agent Menu

Once installed on a machine, the **Antivirus** agent displays a icon in the computer's system tray. This icon provides access to the **Antivirus** agent user interface.

Right clicking the agent icon pops up a menu of options.



- **Kaseya Antivirus** - Displays the **Antivirus** agent user interface.
- **Settings** - Sets all **Antivirus** general protection settings.
- **Pause protection...** - Pauses protection on the machine for a specified time period.
- **About** - Displays the About box for the **Antivirus** agent.
- **Exit** - Terminates the **Antivirus** agent service on the managed machine. The machine is no longer protected by **Antivirus**.

Note: **Customize the user interface of the Antivirus client on the endpoint** *(https://helpdesk.kaseya.com/entries/32410117).*

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** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#209.htm)* and machine groups the user is authorized to see using System > **Scopes** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#4578.htm)*.

Actions

- **Actions**
  - **New** - Creates a new dashboard.

  - **Save** - Saves changes to the currently displayed dashboard.
  - **Save As** - Saves the currently displayed dashboard with a new name.
  - **Delete** - Deletes the currently displayed dashboard.
- **Select Dashboard** - Selects a dashboard to display.
- **Add Parts** - Adds parts to the currently displayed dashboard. See the part list below.
- **Open in Separate Window** - Displays the selected dashboard in a separate tab or window.

Antivirus Dashboard Parts

- **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.
- **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 13)* page.
- **Antivirus Unfiltered License Summary** - A chart displays the number of machines that are `Available`, `Expired`, `In Use`, `Partials` and `Pending Install`.

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** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#209.htm)* and machine groups the user is authorized to see using System > **Scopes** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#4578.htm)*.

Actions

- **Details** - Click to learn more about a selected threat from Kaspersky's Securelist web site.
- **Add Exclusion** - Adds selected rows to the **excluded list** *(page 21)*.
- **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** *(page 10)*.
  - `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 Kaseya **support ticket** *(https://helpdesk.kaseya.com/home)*.
  - `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.

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 machine IDs using Antivirus > **Machines** *(page 3)* > **Assign**. Typically different types of machines or networks require different profiles. 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.

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. Sample profiles of each profile type are provided for you. 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 Workstation 6 Profile`
  - `Kaspersky Server 10 Profile`
  - `Kaspersky Server 6 Profile`

> **Note:** **Antivirus** 6.5 supports both Kaspersky version 10 and legacy version 6, for workstation and server endpoints. Specialized profiles are provided to manage each type of machine. *Kasperksy version 2010 endpoints are not supported in* **Antivirus** *6.5.* **Antivirus** 6.5 only installs or upgrades endpoints to Kaspersky version 10. *Version 10 is strongly recommended.* You can upgrade a Kaspersky version 6 endpoint to Kaspersky version 10 using the Install > **Upgrade Client Version** button on the Control Panel.

- **Open** - Opens an existing profile for editing. You can also double-click a profile to open it.
- **Delete** - Deletes an existing profile.
- **Save** - Saves changes to the currently selected 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.
  - **to Kaspersky 10 Profile** - Copies a selected profile to a Kaspersky version 10 profile.
- **Filter**
  - `Show Kaspersky Workstation Profiles Only`
  - `Show Kaspersky Server Profiles Only`
  - `Show Kaspersky 10.0.0.0 Profiles Only`
  - `Show Kaspersky 6.0.4.1424 Profiles Only`
- **Remove Filter** - Removes the filter.

Adding / Editing Profiles

Click **New**, then a *profile type*, to display the **New Profile** window, or click an existing profile, then click **Open** to display the **Edit Profile** window.

- **Summary tab** *(page 15)*
- **Protection tab** *(page 16)*
- **Quick Scan tab** *(page 19)*
- **Full Scan tab** *(page 20)*
- **Update Options tab** *(page 21)*
- **Exclusions tab** *(page 21)*
- **Endpoints tab** *(page 23)*

Table Columns

- **Name** - Name of the profile.
- **Profile Type** - `Kaspersky File Server` or `Kaspersky Workstation`
- **Machines Applied** - Number of machines using this profile.
- **Created by** - VSA user who created this profile.
- **Version**
  - `6.0.4.1424` or `6.0.4.1611`- Version 6, server or workstation
  - `10.x.x.x` - Kaspersky Endpoint Security for Business, version 10

Summary tab

Antivirus > Configuration > Profiles > Summary tab

> **Note:** Unsupported options for each version of profile are disabled (grayed out).

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

- **Profile Type** - **Antivirus** file server or workstation.
- **Profile Version**
  - `6.0.4.1424` or `6.0.4.1611`- Version 6, server or workstation
  - `10.x.x.x` - Kaspersky Endpoint Security for Business, version 10

Protection tab

Antivirus > Configuration > Profiles > Protection

Note: Unsupported options for each version of profile are disabled (grayed out).

Options

- **Enable Protection** - If checked, all protection components selected for this profile are enabled.
- **Launch Antivirus at computer startup** - If checked, all protection components selected for this profile are enabled at startup.
- **Enable Self-Defense** - Prevents unauthorized access to **Antivirus** files, including protection against auto-clickers.

Interactive Protection

- **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.
  - **Do not delete suspicious objects** - If checked and actions are automatically applied, suspicious objects are not deleted.
- **Show the "Protected by Kaspersky Lab" on the Microsoft Windows Logon Screen** - If checked, shows the label.
- **Show icon in the taskbar** - If checked, the **Antivirus** client's icon displays in the system tray of the user's computer. The user can click or right-click the icon to access the **Antivirus Agent Menu** *(page 12)*.
- **Show in the 'Start' menu** - If checked, the **Antivirus** client displays as a program in the user's Start menu.
- **Show in the "Add or Remove Programs" ("Programs and Features") list** - If checked, the **Antivirus** client displays as a program in the user's Add or Remove Programs list. The user can uninstall the **Antivirus** client.

Note: For each component lists below, corresponding icons display in the **Component Status** field of the **Details Panel** *(page 10)* of the **Machines** page.

File Antivirus

Applies to workstations and servers.

- **Enable File Antivirus** - If checked, scans all files that are opened, saved, or executed.
- **Scan New and Changed Files Only** - If checked, scans only new files and files modified since the last scan.
- **Protect Network Drives** - If checked, includes mapped network drives.
- **Protect Removable Drives** - If checked, includes removable drives.
- **Scan Archives** - If checked, scans archived files.
- **Scan Installation Packages** - If checked, scans installation packages.

- **Scan Embedded OLE Objects** - If checked, scans OLE objects embedded within files.
- **Heuristics Analysis** - If checked, uses heuristics analysis to identify the behavior of objects as malicious or suspicious, even if they are not yet identified an 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`.
- **Extract Compound Files in the Background** - If checked, compound files larger than the size specified by **Minimum Files 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.
- **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

Applies to workstations only.

- **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.
- **Check incoming messages only** - If checked, only incoming email is scanned. If blank, both incoming and outgoing email is scanned.
- **POP3/SMTP/NMTP/IMAP Traffic** - If checked, scans POP3/SMTP/NMTP/IMAP email traffic.
- **ICQ/MSN Traffic** - If checked, scans ICQ and MSN instant messaging 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!
- **Check if URLs are listed in the base of suspicious web-addresses** - If checked, scans the links of email messages included in the database of suspicious web addresses.
- **Check if URLs are listed in the base of phishing web-addresses** - If checked, scans the links of email messages included in the database of phishing web addresses.
- **Heuristics Analysis** - If checked, uses heuristics analysis to identify the behavior of objects as malicious or suspicious, even if they are not yet identified an 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

Applies to workstations only.

- **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.
- **Check if URLs are listed in the base of suspicious web-addresses** - If checked, scans the links of email messages included in the database of suspicious web addresses.
- **Check if URLs are listed in the base of phishing web-addresses** - If checked, scans the links of email messages included in the database of phishing web addresses.
- **Limit fragment 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 fragment caching causes slow browsers and HTTP connections to time out.
- **Caching time in seconds** - Specifies the time limit for fragment caching.
- **Heuristics Analysis** - If checked, uses heuristics analysis to identify the behavior of objects as malicious or suspicious, even if they are not yet identified an 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`.

IM Antivirus

Applies to workstations only.

- **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.

Proactive Antivirus

Applies to workstations only.

- **Enable Proactive Antivirus** - If checked, recognizes a new threat on your computer by the sequence of actions executed by a program. If the sequence of application's actions arouses any suspicion, **Antivirus** blocks the activity of this application.
- **Enable Application Activity Monitor** - If checked, application activity on a computer is monitored for suspicious events.
- **Enable Registry Guard** - If checked, protects the registry from suspicious changes to critical applications.

Access Control

Applies to workstations only.

- **Enable Access Control** - If checked, prevents autorun access.
- **Disable autorun for all devices** - If checked, disables autorunning of applications and devices on removable media connected to the computer.
- **Disable processing autorun.inf** - If checked, disables autorunning of `autorun.inf` files.

Anti-Spy

Applies to workstations only.

- **Enable Anti-Spy** - If checked, intercepts dialers attempting to establish a connection with pay-per-use websites and blocks them.
- **Enable Anti Banner** - If checked, blocks advertisements on special banners on the web or built into the interfaces of various programs installed on your computer.
- **Enable Anti Dialer** - If checked, a popup window notifies the user that a secret connection is being attempted on the user's computer to dial a connection to a phone number. The user is given the option of blocking or allowing the connection.

Anti-Spam

Applies to workstations only.

- **Enable Anti-Spam** - If checked, integrates with the mail client installed on your computer, and monitors all incoming email messages for spam. All messages containing spam are marked with a special header. The component also analyzes email messages to detect phishing.
- **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 anti-spam options using the **Tools > Options > Anti-Spam** tab in Outlook.
- **Additional: Microsoft Outlook Express Plug-in** - If checked, installs a plugin for the Outlook Express email client that enables the configuration of anti-spam options. A special window opens when you click the **Settings** button near the **Spam** and **Not Spam** buttons on the taskbar of Outlook Express.
- **Additional: The Bat! Plug-in** - If checked, installs a plugin for The Bat! email client that enables the configuration of anti-spam options using the **Properties > Settings > Spam protection** item in The Bat!
- **Open Mail Dispatcher when receiving email via POP3** - If checked, the user can preview email stored on a POP3 server in a **Dispatcher** window before downloading the email to the local computer. This reduces the risk of downloading spam or viruses.
- **Train on outgoing mail** - If checked, the email addresses of the first 50 outgoing emails sent by the user after this option is enabled are added to the user's white list. The white list is a list of trusted email addresses and phrases that classify email as useful.
- **Do not check Microsoft Exchange Server native messages** - If checked, does not scan email sent internally by the user's own Microsoft Exchange Server.
- **Check if URLs are listed in the base of suspicious web-addresses** - If checked, scans the links of email messages included in the database of suspicious web addresses.
- **Check if URLs are listed in the base of phishing web-addresses** - If checked, scans the links of email messages included in the database of phishing web addresses.

Network Options

- **Kaspersky will monitor the following ports (comma delimited)** - Specifies the list of network ports monitored by the Mail Antivirus, Web Antivirus, and IM Antivirus components.

Quick Scan / Critical Scan tab

Antivirus > Configuration > Profiles > Quick Scan or Critical Scan

Note: Unsupported options for each version of profile are disabled (grayed out).

Note: Quick Scan was renamed to Critical Scan starting with **Antivirus** version 10.x

An **Antivirus quick scan / critical scan** scans operating system startup objects.

- **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.
- **Schedule**
  - **Manually** - Scans of machines using this profile are only scheduled manually.

- **By schedule / Scan Run time / Run every** - Schedules scans of machines using this profile by the specified number of time periods. Time is agent-based.
- **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.
- **Pause scheduled scans when screensaver is inactive or computer is unlocked** - If checked, scanning is paused when the computer is being used.
- **Prompt for action when scan is complete** - If checked and a threat is detected during the scan, the user is prompted at the *end* of the scan whether to disinfect quarantined files. If disinfect fails the user is also prompted whether to delete quarantined files.
- **Prompt for action during scan** - If checked and a threat is detected *during* the scan, the user is prompted during the scan whether to disinfect a quarantined file, and if disinfect fails whether to delete the quarantined file.
- **Do not prompt for action** - The user is not prompted if a threat is detected.
  - ✓ **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.
- **Concede Resources To Other Applications** - If checked, when the load on the file system from other applications increases, scan tasks will pause their activity.

Full Scan tab

Antivirus > Configuration > Profiles > Full Scan

Note: Unsupported options for each version of profile are disabled (grayed out).

A **full scan** performs a thorough **Antivirus** 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.

- **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.
- **Schedule**
  - **Manually** - Scans of machines using this profile are only scheduled manually.
  - **By schedule / Scan Run time** - Schedules scans of machines using this profile by the specified number of time periods. Time is agent-based.
  - **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.
  - **Pause scheduled scans when screensaver is inactive or computer is unlocked** - If checked, scanning is paused when the computer is being used.
  - **Prompt for action when scan is complete** - If checked and a threat is detected during the scan, the user is prompted at the *end* of the scan whether to disinfect quarantined files. If disinfect fails the user is also prompted whether to delete quarantined files.

- **Prompt for action during scan** - If checked and a threat is detected *during* the scan, the user is prompted during the scan whether to disinfect a quarantined file, and if disinfect fails whether to delete the quarantined file.
- **Do not prompt for action** - The user is not prompted if a threat is detected.
  - ✓ **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.
- **Concede Resources To Other Applications** - If checked, when the load on the file system from other applications increases, scan tasks will pause their activity.

Update Options tab

Antivirus > Configuration > Profiles > Update Options

Note: Unsupported options for each version of profile are disabled (grayed out).

The **Update Options** 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 3)* page.
- **By schedule / Update Run time / Run every** - Schedules updates of the **Antivirus** client and its definitions database on all **Antivirus** managed machines using this profile by the specified number of time periods. Time is agent-based.
- **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.

Proxy Settings

Specify a proxy server if client machines require one to download **Antivirus** updates from the web.

- **Use custom proxy server settings** - 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** - If **Specify Authentication Data** is checked, enter a valid username.
  - **Encrypted Password** - If **Specify Authentication Data** is checked, enter a valid password.
- **Bypass proxy server for local addresses** - If checked, local IP addresses do not use the proxy server.

Exclusions tab

Antivirus > Configuration > Profiles > Exclusions

Note: Unsupported options for each version of profile are disabled (grayed out).

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

Exclusion Rules

- **Add Exclusion** - 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
  - `*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.

- **Add Trusted App** - 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** *(page 16)*.

- **Add Trusted URL** - 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.kaseya.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.kaseya.com/test\?`

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** *(page 12)* > **Alert Profiles**. Different types of machines may require different alert profiles. Alert profiles are visible to all VSA users.

Note: Alert profiles created in either **Antivirus** or **AntiMalware** are visible and editable in both products. If a machine is assigned an alert profile using either **Antivirus** or **AntiMalware**, the alert profile is assigned to both products on that machine.

Reviewing Alarms Created by Antivirus Alerts

- Monitor > **Alarm Summary** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#1959.htm)*
- Monitor > Dashboard List > any **Alarm Summary Window** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#4112.htm)* within a dashlet
- Agent > Agent Logs > **Agent Log** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#354.htm)*
- The Agent > Agent Logs > **Monitor Action Log** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#354.htm)* - Shows the actions taken in response to an alert, whether or not an alarm was created.
- **Live Connect** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#4796.htm)* > Agent Data > Agent Logs > Alarm Log
- Info Center > Reporting > Legacy Reports > Logs > Alarm Log

Actions

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

Adding / Editing Profiles

Click **New** to display the **New Alert Profile** window, or click an existing profile, then click **Open** to display the **Edit Alert Profile** window.

- Summary tab
- Alert Types tab
- Actions tab
- **Endpoints tab** *(page 25)*

Table Columns

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

Summary tab

Antivirus > Configuration > Alerts > Summary tab

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

Alert Types tab

Antivirus > Configuration > Alerts > Alert Types tab

Select Alerts and Configuration Data

- **Security 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 be 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 13)* 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.
- **License expiring in X days / Number of days** - A license is expiring in a specified number of days.
- **License expired and not renewed** - A managed security product's license is expired and is not renewed.
- **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 manage security product repair failed.
- **Client uninstall failed** - A managed security product uninstall failed.

Actions tab

Antivirus > Configuration > Alerts > Actions tab

The **Actions** tab of an alert profile determines the actions taken in response to any of the **Alert Types** *(page 24)* 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.
- **Run Script** - If checked and an alert condition is encountered, an agent procedure is run.

  - **Script Name** - Select the name of the agent procedure.
- **Send Message to Info Center** - If checked and an alert condition is encountered, an email is sent to the specified email addresses.
  - **Select Users to Notify** - Select the users to notify about **Antivirus** alerts using the Info Center > **Inbox** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#9460.htm)*.
- **Send Message to Notification Bar** - If checked and an alert condition is encountered, an email is sent to the specified email addresses.
  - **Select Users to Notify** - Select the users to notify about **Antivirus** alerts using the **Notification Bar** *(http://help.kaseya.com/webhelp/EN/VSA/9010000/index.asp#10634.htm)*.

Endpoints tab

Endpoint Protection > Configuration > Alerts > Endpoints

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

Note: The Machines > Details > **Alert Profiles** tab displays the list of alert profiles assigned to a selected machine.

Index

A

Actions tab • 24
Alert Types tab • 24
Alerts • 23
Antivirus Agent Menu • 12
Antivirus Columns • 9
Antivirus Module Requirements • 3
Antivirus Overview • 1

C

Control Panel • 6

D

Dashboards • 12
Details Panel • 10
Detections • 13

E

Endpoints tab • 23, 25
Exclusions tab • 21
Explorer Grid • 4

F

Full Scan tab • 20

M

Machines • 3

P

Page Layout • 4
Profiles • 14
Protection tab • 16

Q

Quick Scan / Critical Scan tab • 19

S

Summary tab • 15, 24

U

Update Options tab • 21