Anti-Malware

User Guide

Version R95

English

February 4, 2021

Copyright 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

Contents

Anti-Malware Overview

Note: The module previously called *Anti-Malware* in 9.2 is now called **Anti-Malware (Classic)** in 9.3 and later versions. Upgrading the VSA to 9.3 or later causes agent machines installed with the MalwareBytes client to continue to be managed using **Anti-Malware (Classic)** just as they were before in earlier releases. Starting with 9.3 an enhanced **Anti-Malware** module was made available and is recommended over the older product. To migrate agents from **Anti-Malware (Classic)** to the enhanced **Anti-Malware** module, reinstall over the existing installation of MalwareBytes from the enhanced **Anti-Malware** module. Profile settings are not migrated. Contact support if you would like assistance migrating profile settings.

Anti-Malware provides Malwarebytes' Anti-Malware Pro endpoint security for managed machines. **Anti-Malware** can be installed independently of **Endpoint Security** or **Antivirus**. **Anti-Malware** is particularly adept at detecting and preventing *ScareWare* or *Rogue Antivirus* spyware that installs a virus, then attempts to bill the user to remove it.

Anti-Malware quickly detects, destroys, and blocks malicious software. Every process is monitored and malicious processes are stopped before they even start. Scanning and realtime protection both use advanced heuristic scanning technology to keep systems safe and secure against even the latest malware threats.

- Support for Windows 7, 8 and 8.1 (32-bit and 64-bit). Does not support servers.
- Light speed quick scanning.
- Ability to perform full scans for all drives.
- Database updates released daily protect against the newest malware in-the-wild.
- Intelligent heuristics detect even the most persistent malware while remaining light on system resources.
- Realtime protection monitors filesystem and internet traffic.
- Scheduler to keep protection up-to-date automatically.
- Quarantine to hold threats and restore them at your convenience.
- Ignore list for both the scanner and the protection module.
- Threats are quarantined automatically.
- Protection controls entire machine, beyond individual accounts.
- Supports exclusions of files, folders, registry keys and values, and IP4 addresses.
- **Policy Management** *(http://help.kaseya.com/webhelp/EN/KPM/9050000/index.asp#34012.htm)* can manage the installation of the **Anti-Malware** client and the assignment of **Anti-Malware** profiles and alert profiles.
- Peer-to-peer file downloading automatically fetches Anti-Malware files from other endpoints on the same local network, if these files have already been downloaded.

Note: See **Anti-Malware System Requirements** *(page iii)*.

Functions	Description
Machines *(page 5)*	Installs and uninstalls Anti-Malware software on selected machines and provides a detailed view of the Anti-Malware status of any selected machine.
Dashboards *(page 12)*	Displays a dashboard view of the status of all machines installed with Anti-Malware.
Detections *(page 12)*	Displays virus threats you can take action on.
Profiles *(page 15)*	Manages Anti-Malware profiles that are assigned to

	machine IDs.
Alerts *(page 21)*	Manages Anti-Malware module alerts.
Settings	Maintains module-level preferences.
Application Logging	Displays a log of Antivirus module activity.

Anti-Malware Module Minimum Requirements

Kaseya Server

- The Anti-Malware R95 module requires VSA R95.

Requirements for Each Managed Machine

- 800MHZ processor.
- 2048 MB of RAM.
- 25 MB free disk space.
- Microsoft Windows 8, 8.1, 10.
- Microsoft Windows Server 2012/2012 R2, 2016.
- MacOS and Linux are not supported.
- See Malwarebytes **system requirements** *(https://www.malwarebytes.org/business/antimalware/)* for more information.

Note: See general **System Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9050000/reqs/index.asp#home.htm).*

Chapter 1

Show

In This Chapter

Machines

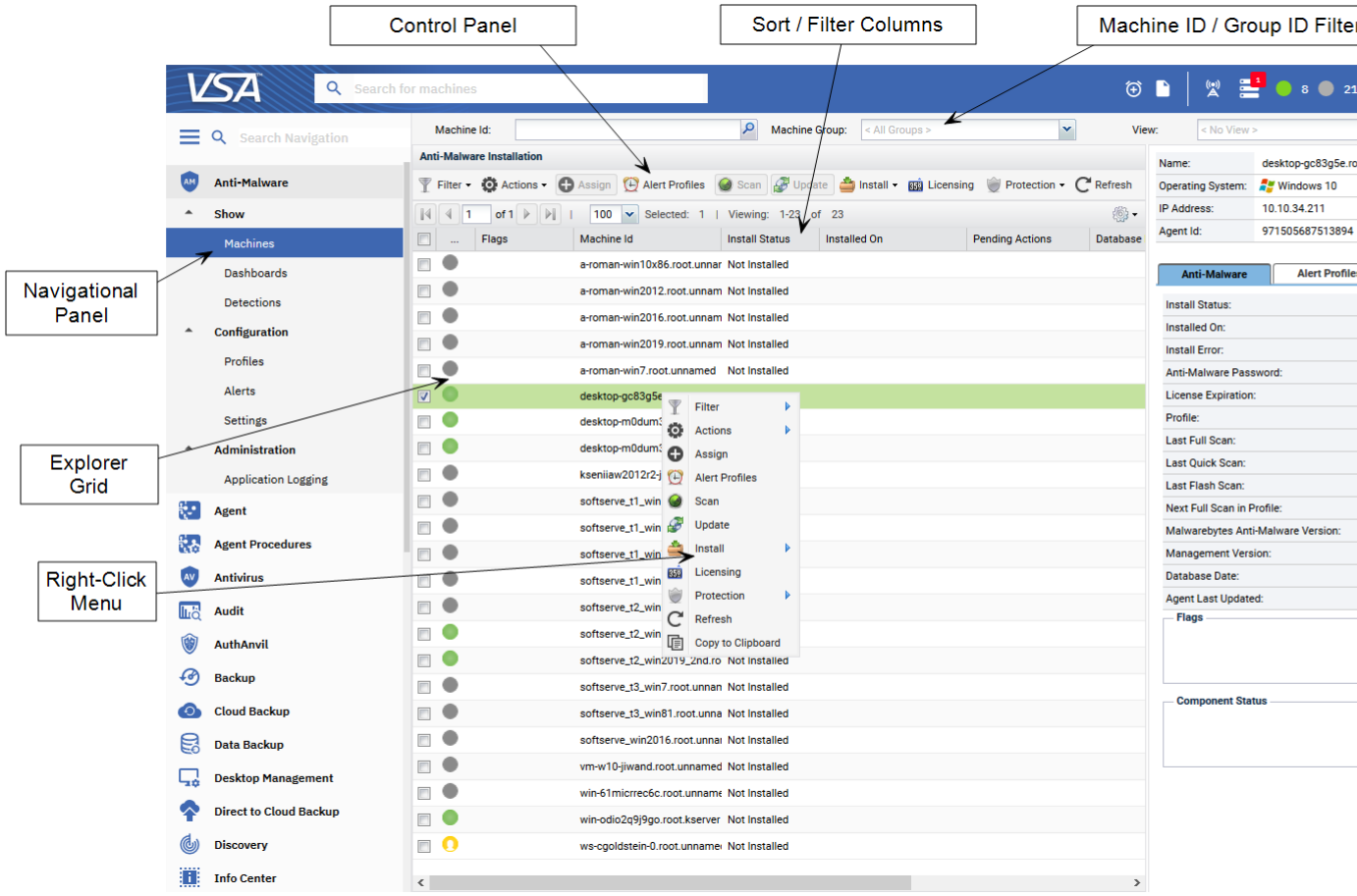
Anti-Malware > Show > Manage Machines

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

In This Section

Page Layout

The layout of the **Machines** *(page 5)* page comprises the following design elements:



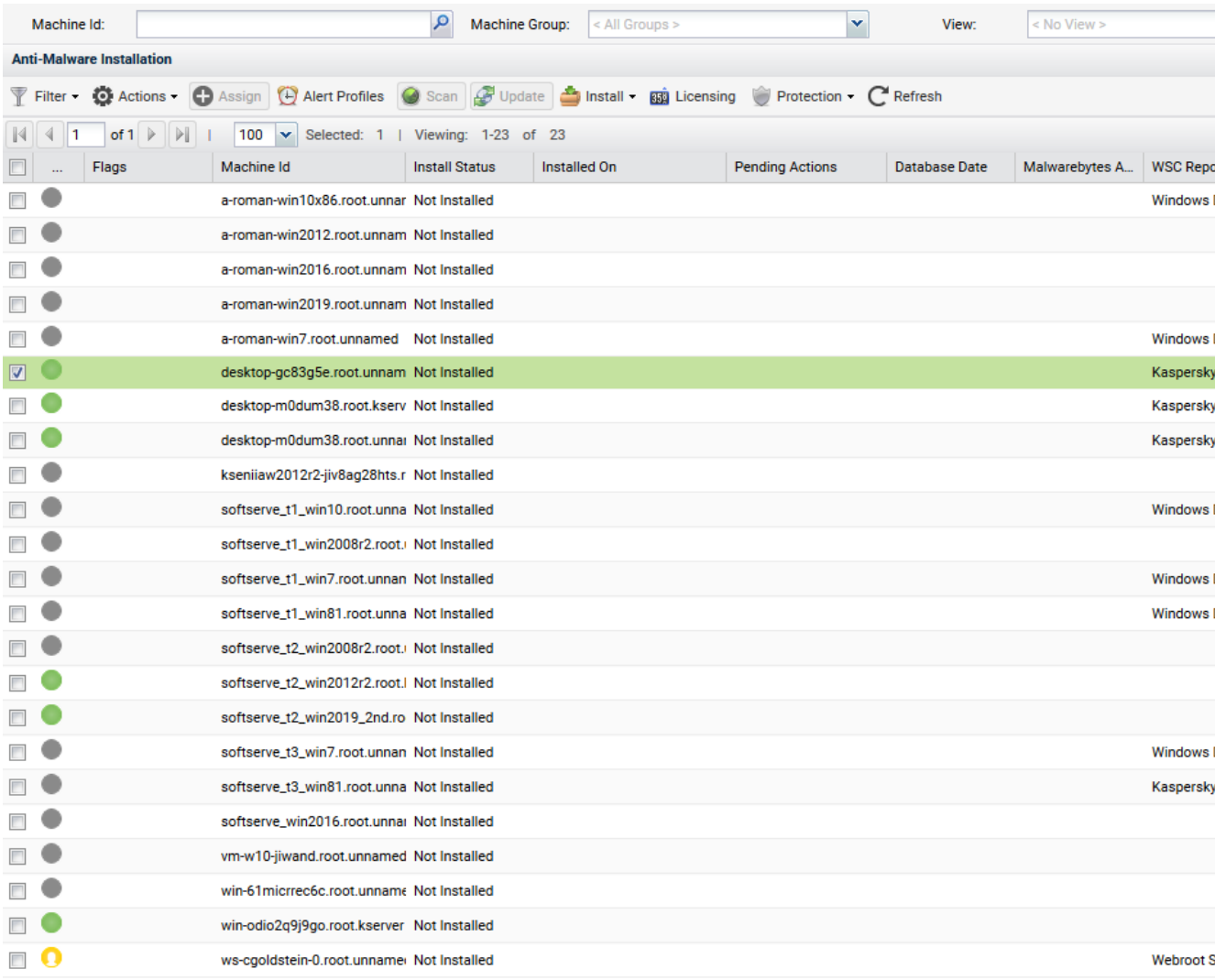
- **Navigation Panel** - Used to navigate to pages within the **Anti-Malware** module.
- **Explorer Grid** - Each managed machine in the VSA is listed in this panel.
  - **Page Browser** - If more than one page of devices displays, pages forwards and back.
  - **Rows Per Page** - Sets the number of devices 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**.
  - **Anti-Malware** - Displays a summary of the **Anti-Malware** 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 5)* page lists all agent machines your current scope and **machine ID / group ID filter** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#209.htm)* permit you to see. Additional columns display information about machines installed with **Anti-Malware**.

- 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
	scan in progress
	license expired
	endpoint configuration out of compliance with the profile
	pending enable
	pending disable
	scan pending
	uninstall pending
	repair pending

	install pending
	update profile pending profile assignment pending
	update pending
	install failed

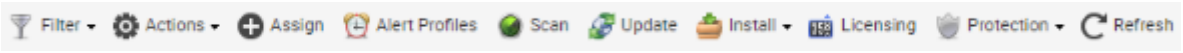
Component Icon Conventions

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.

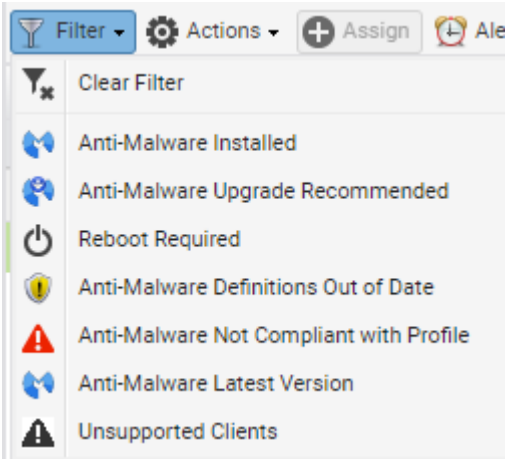
Status	Type of Icon Displayed	Example: File Protection Icons
Disabled	grey X mark	
Failure	yellow exclamation point	
Running/Enabled	green checkmark	
Starting	a key with a green arrow	
Stopped	red X mark	
Stopping	a key with a red minus sign	

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 any of the selected filters. **Anti-Malware Installed**
- **Anti-Malware Upgrade Recommended** - Helps you identify which machines are eligible for upgrading to the latest version. To upgrade, install over an existing installation of **Anti-Malware**.

- **Reboot Required**
- **Anti-Malware Definitions Out of Date**
- **Anti-Malware Not Compliant with Profile**
- **Anti-Malware Latest Version**
- **Unsupported Clients**

Gear

- **Export** - Exports the grid to a CSV file.
- **Refresh** - Refreshes the grid.
- **Reset Filter** - Clears the grid of any selected filters.

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 **Anti-Malware** configuration profile to selected machines. 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 **Anti-Malware** scan on selected machines.

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

For **Anti-Malware** there are three types of scan:

- **Full Scan** - A full scan scans all files on the selected drives. A quick scan is recommended in most cases.
- **Quick Scan** - A quick scan uses fast scanning technology to scan systems for malicious software.
- **Flash Scan** - A flash scan analyzes memory and auto-run objects.

Update

Schedules an update on selected machines with the latest **Anti-Malware** definitions.

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

Install

- **Install or Upgrade Anti-Malware** - Installs or upgrades the **Anti-Malware** client on selected machines.
  - **Anti-Malware Profile** - The profile to be applied after installation.
  - **Advanced Options**
    - ✓ **Start Date & Time** - The start date and start time of the install.

      Note: The scheduling of installs, updates, scans, uninstalls, and repairs are automatically staggered when multiple machines are tasked concurrently. This applies to both on premises VSAs and across all VSA tenant partitions on the same SaaS server.

    - ✓ **Allow Reboot** - If checked, allows a reboot if necessary.
    - ✓ **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 **Anti-Malware** using **Policy Management** *(http://help.kaseya.com/webhelp/EN/KPM/9050000/index.asp#34012.htm)*. 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 Anti-Malware** - Uninstalls the **Anti-Malware** client on selected machines.
  - **Start Date & Time** - The start date of the uninstall.
  - **Allow Reboot** - If checked, allows a reboot if necessary.
- **Repair Anti-Malware Install** - Re-installs missing files on a previously installed **Anti-Malware** client to repair it. The **Anti-Malware** client must have been previously installed using **Anti-Malware** for the same VSA.
  - **Start Date & Time** - The start date and start time of the repairl.
  - **Allow Reboot** - If checked, allows a reboot if necessary.

Licensing

Licensing sets the expiration date for all KAV, KAM, and KES client licenses purchased equal to the VSA maintenance expiration date.

- **License Counts** - Lists **Anti-Malware** license counts. **Anti-Malware** license counts also display on the Administration > Manage > **License Manage** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#2924.htm)* page.
  - `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 **Anti-Malware** 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 Anti-Malware** - Re-enables **Anti-Malware** protection on selected machines.
- **Temporarily Disable Anti-Malware** - Disables **Anti-Malware** protection on selected machines. Some software installations require **Anti-Malware** software be disabled to complete the install.

Columns

All columns support **selectable columns, column sorting, column filtering and flexible columns widths** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#6875.htm)*.

Selectable Columns

- **Agent Id -** The unique GUID of the Kaseya 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 VSA.
- **Install Status** - `Not Installed`, `Script Scheduled`, `Installed`, `Installed (Classic AM)`
- **Installed On** - The date **Anti-Malware** was installed.
- **Pending Actions** - `Install`, `Assign`, `Update`, `Scan`. Clicking the pending action  icon during an install displays the following action statuses: `Downloading Files`, `Installing`, `Downloading OEM files to the VSA`, `Downloading Files to the endpoint`, `Installing product on the endpoint`.

- **Database Date** - The date and time the **Anti-Malware** definition database was last updated.
- **Malwarebytes Anti-Malware Version** - The version number of the Malwarebytes client installed on this machine.
- **WSC Reported Product Name** - The name of the security product registered with *Windows Security Center*.
- **AM Profile** - The **Anti-Malware** profile assigned to this machine.
- **AM Components** - Identifies the status of **Anti-Malware** components installed on this machine.
- **Has Active Threats** - Number of detections that could not be automatically disinfected or deleted and require user attention.
- **Last Full Scan** - The last date and time all files on selected drives were scanned using **Anti-Malware**.
- **Last Flash Scan** - The last date and time a flash scan analyzed memory and auto-run objects using **Anti-Malware**.
- **Last Quick Scan** - The last date and time a quick scan for malicious software was performed using **Anti-Malware**.
- **Last Reboot** - The date/time the machine was last rebooted.
- **Login Name** - The currently logged on user.
- **Management Version** - The version of the Kaseya agent.
- **Next Full Scan in Profile** - 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** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#503.htm)*.
- **WSC Manufacturer** - The manufacturer of the WSC reported product.

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

- **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 **Anti-Malware** was installed.
- **Install Error** - If an install error occurs, displays a description of the error.
- **Anti-Malware Password** - The password required to reconfigure or uninstall the Malwarebytes client.
- **License Expiration** - The date **Anti-Malware** security is scheduled to expire.
- **Profile** - The **Anti-Malware** configuration **profile** *(page 15)* assigned to this machine.
- **Last Full Scan** - The last date and time all files on selected drives were scanned using **Anti-Malware**.
- **Last Quick Scan** - The last date and time a quick scan for malicious software was performed using **Anti-Malware**.

- **Last Flash Scan** - The last date and time a flash scan analyzed memory and auto-run objects using **Anti-Malware**.
- **Next Full Scan in Profile** - Calculates the next full scan from the scheduled tasks section of the assigned profile.
- **Malwarebytes Anti-Malware Version** - The version number of the Malwarebytes client installed on this machine.
- **Management Version** - The version of the Kaseya agent.
- **Database Date** - The date and time the **Anti-Malware** definition database was last updated.
- **Agent Last Updated** - The date and time the **Anti-Malware** client was last updated.
- **Flags** - Possible flags include: `Definitions out of date`, `Out of Compliance`.
- **Component Status** - Identifies the status of **Anti-Malware** components installed on this machine.

 - File Execution Blocking is running or stopped.

 - Malicious website blocking is running or stopped.

Alert Profiles tab

Displays the list of **alert profiles** *(page 21)* assigned to the selected machine.

> **Note:** The Alerts > (profile) > **Endpoints** *(page 23)* tab lists all machines using a selected alerts profile.

Dashboards

Anti-Malware > Show > Dashboards

The **Dashboards** page provides a dashboard view of the status of machines installed with **Anti-Malware**. The dashboard statistics displayed depends on the **machine ID / group ID filter** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#209.htm)* and machine groups the user is authorized to see using System > **Scopes** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#4578.htm)*.

- **Anti-Malware Protection Status** - A pie chart displays percentage categories of machines with **Anti-Malware** protection. Percentage categories include `Not Installed`, `Out of Date`, `Not Enabled`, and `Up to Date`.
- **Anti-Malware 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 12)* page.
- **Anti-Malware Unfiltered License Summary** - A chart displays the number of machines that are `Available`, `Expired`, `In Use`, `Partials` and `Pending Install`.
- **Anti-Malware Machines Needing Attention** - A bar chart displays the number of **Anti-Malware** managed machines needing attention, by category. Categories include `No AM Installed`, `Uncured Threats`, `Out of Date`, `Reboot Needed`, `Component`.
- **Anti-Malware Number of Machines with Detections** - A bar chart displays the number of detections.

Detections

Anti-Malware > Show > Manage Detections

The **Detections** page displays virus threats not automatically resolved by **Anti-Malware**. 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/9050000/index.asp#209.htm)* and machine groups the user is authorized

to see using System > **Scopes** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#4578.htm)*.

Actions

- **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:
  - **Clear Filter** - Removes all filtering from the list.
  - **Active Threats** - Displays **Anti-Malware** 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.

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:
  - *Detection by Scanner*
    - ✓ `Failed to unload process` - A reboot is probably needed to complete the removal of malware.
    - ✓ `Unloaded process successfully`
    - ✓ `Delete on reboot` - A reboot is needed to complete the removal of malware.
    - ✓ `Quarantined and deleted successfully`
    - ✓ `Not selected for removal` - The item was not selected and probably is not a threat.
  - *Detection by Protection Module*
    - ✓ `ALLOW` - User has clicked **Ignore** on a malware detection.
    - ✓ `QUARANTINE` - User has clicked **Quarantine** on a malware detection
    - ✓ `DENY` - User has clicked **Quarantine** on a malware detection but the blocking was unsuccessful or detection already blocked.
- **Type** - The category of threat.
- **Profile Name** - The name of the profile in use when this threat was detected.

Chapter 2

Configuration

In This Chapter

Profiles

Anti-Malware > Configuration > Profiles

The **Profiles** page manages **Anti-Malware** profiles. Each profile represents a different set of enabled or disabled **Anti-Malware** options. Changes to a profile affect all machine IDs assigned that profile. A profile is assigned to machine IDs using Anti-Malware > **Machines** *(page 5)* > **Assign**. Typically different types of machines or networks require different profiles. Profiles are public by default but can be made **private** *(page 24)*. System profiles are provided and cannot be edited or deleted. Use the Settings > **Application Settings** *(page 24)* tab to make profiles private.

Actions

- **New Profile** - Creates a new configuration profile. Profiles support Malwarebytes Anti-Malware versions 1.80.0.1010
- **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.

Table Columns

- **Name** - Name of the profile.
- **Description** - A description of the profile.
- **Machines** - Number of machines using this profile.
- **Product Version** - `KAM 1.80.2.1012`
- **(Created by)** - (user) or (system)
- **Created Date**
- **Last Updated By**
- **Last Updated**
- **Used in a Policy**

In This Section

Profile Details tab

Anti-Malware > 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** - `Malwarebytes Anti-Malware Profile`
- **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

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

The **Protection** tab sets protection options for a selected **Anti-Malware** profile.

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.

Settings

- **Start Anti-Malware on Computer Startup** - If checked, start protection module when Windows starts.
-  **Start file execution blocking, when protection module starts** - If checked, start file execution blocking when protection module starts.
-  - **Start malicious website blocking when protection module starts** - If checked, start malicious website blocking when protection module starts.
- **Automatically quarantine filesystem threats detected by the protection module** - If checked, quarantines infected files detected by the protection module automatically. If unchecked, the is prompted to take one of three actions: 'Quarantine', 'Allow Temporarily' one time only, or 'Allow Always' which adds the threat to the Ignore List.
- **Show tooltip balloon when filesystem threat is blocked** - If checked, detects and blocks malicious processes and prompts the user to take action upon detection.
- **Show tooltip balloon when malicious website is blocked** - If checked, a tooltip balloon displays to the user when a malicious website is blocked.

Chapter 3

Scheduled Tasks tab

In This Chapter

Quick Scan tab

Anti-Malware > Configuration > Profiles > Scheduled Tasks > Quick Scan

The **Quick Scan** tab schedules recurring quick scans for a selected **Anti-Malware** profile. A quick scan uses fast scanning technology to scan systems for malicious software.

Schedule

- **Type**
  - `Manually` - Updates of machines using this profile are only scheduled manually. Update machines manually using the control panel of the **Machines** *(page 5)* 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** - `Once`, `Hourly`, `Daily`, `Weekly`, `Monthly`, `On Reboot`
  - If `Hourly` is selected, **Run Every X Hours** displays.
  - If `Daily` is selected, **Run Every X Days** displays.
  - If `Weekly` is selected, **Run Every X Weeks** displays.
  - If `Monthly` is selected, **Run Every X Months** displays.
  - If `Once`, `Daily`, `Weekly`, `Monthly` is selected, **Start Date & Time** displays.
- **Recover if missed after X hours** - Runs the scan if the scheduled time was missed, after the specified number of hours has elapsed.

Options

- **Wake from sleep** - If checked, attempts to wake the computer from sleep to perform a scheduled scan.
- **Restart the computer if needed as part of threat removal** - If checked, restarts the computer to complete the removal of threats, if necessary.
- **Automatically remove threats** - If checked, automatically removes threats.

Full Scan tab

Anti-Malware > Configuration > Profiles > Scheduled Tasks > Full Scan

The **Full Scan** tab schedules recurring quick scans for a selected **Anti-Malware** profile. A full scan scans all files on the selected drives. A quick scan is recommended in most cases.

Schedule

- **Type**

- `Manually` - Updates of machines using this profile are only scheduled manually. Update machines manually using the control panel of the **Machines** *(page 5)* 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** - `Once`, `Hourly`, `Daily`, `Weekly`, `Monthly`, `On Reboot`
  - If `Hourly` is selected, **Run Every X Hours** displays.
  - If `Daily` is selected, **Run Every X Days** displays.
  - If `Weekly` is selected, **Run Every X Weeks** displays.
  - If `Monthly` is selected, **Run Every X Months** displays.
  - If `Once`, `Daily`, `Weekly`, `Monthly` is selected, **Start Date & Time** displays.
- **Recover if missed after X hours** - Runs the scan if the scheduled time was missed, after the specified number of hours has elapsed.

Options

- **Wake from sleep** - If checked, attempts to wake the computer from sleep to perform a scheduled scan.
- **Restart the computer if needed as part of threat removal** - If checked, restarts the computer to complete the removal of threats, if necessary.
- **Automatically remove threats** - If checked, automatically removes threats.

Flash Scan tab

`Anti-Malware > Configuration > Profiles > Scheduled Tasks > Flash Scan`

The **Flash Scan** tab schedules recurring quick scans for a selected **Anti-Malware** profile. A flash scan analyzes memory and auto-run objects.

Schedule

- **Type**
  - `Manually` - Updates of machines using this profile are only scheduled manually. Update machines manually using the control panel of the **Machines** *(page 5)* 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** - `Once`, `Hourly`, `Daily`, `Weekly`, `Monthly`, `On Reboot`
  - If `Hourly` is selected, **Run Every X Hours** displays.
  - If `Daily` is selected, **Run Every X Days** displays.
  - If `Weekly` is selected, **Run Every X Weeks** displays.
  - If `Monthly` is selected, **Run Every X Months** displays.
  - If `Once`, `Daily`, `Weekly`, `Monthly` is selected, **Start Date & Time** displays.
- **Recover if missed after X hours** - Runs the scan if the scheduled time was missed, after the specified number of hours has elapsed.

Options

- **Wake from sleep** - If checked, attempts to wake the computer from sleep to perform a scheduled scan.
- **Restart the computer if needed as part of threat removal** - If checked, restarts the computer to complete the removal of threats, if necessary.
- **Automatically remove threats** - If checked, automatically removes threats.

Update tab

Anti-Malware > Configuration > Profiles > Scheduled Tasks > Update Options

The **Update** tab schedules the downloading of **Anti-Malware** updates to client machines for a selected profile.

Schedule

- **Type**
  - `Manually` - Updates of machines using this profile are only scheduled manually. Update machines manually using the control panel of the **Machines** *(page 5)* 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** - `Once`, `Hourly`, `Daily`, `Weekly`, `Monthly`, `On Reboot`
  - If `Hourly` is selected, **Run Every X Hours** displays.
  - If `Daily` is selected, **Run Every X Days** displays.
  - If `Weekly` is selected, **Run Every X Weeks** displays.
  - If `Monthly` is selected, **Run Every X Months** displays.
  - If `Once`, `Daily`, `Weekly`, `Monthly` is selected, **Start Date & Time** displays.
- **Recover if missed after X hours** - Runs the scan if the scheduled time was missed, after the specified number of hours has elapsed.

Options

- **Wake from sleep** - If checked, the machine will be wakened, if necessary, to perform the update.
- **Run flash scan after successful update** - If checked, runs a flash scan just after the update.

Exclusions tab

Anti-Malware > Configuration > Profiles > New/Edit > Exclusions

The **Exclusions** tab for **Anti-Malware** profiles excludes objects from **Anti-Malware** monitoring.

Include Global Settings - If checked, **Global Exclusions** *(page 23)* are enabled for this profile.

Exclusion Rules

- **New** - Adds entries to be excluded from scanning and protection, up to a limit of 256 exclusions. Wildcards are not supported.
  - Type - Select type from the drop-down: File, Folder, IPv4, Registry Key, Registry Value.
  - Path - Path must begin with a drive letter. Examples: `C:\Windows\file.exe` or `C:\Windows\folder`.
- **Delete** - Deletes a selected exclusion rule.

Advanced Settings tab

Anti-Malware > Configuration > Profiles > New or Edit > Advanced Settings

General Settings Tab

Settings

- **Terminate Internet Explorer during threat removal** - If checked, terminates Internet Explorer browsing sessions automatically before removing threats detected in the Temporary Internet Files folder. If unchecked, a reboot may be required to complete the threat removal process.

- **Report anonymous usage statistics** - If checked, reports usage statistics to MalwareBytes. No personal information is collected.
- **Create right click context menu** - If checked, the machine user may right-click a file or folder to scan that file or folder.

Database

- **Warn if database is outdated** - If checked, notifies the VSA user the database update has not occurred within the specified number of days.

Install Procedures

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

Uninstall Procedures

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

Scanner Settings tab

- Scan memory objects
- Scan startup objects
- Scan registry objects
- Scan filesystem objects
- Scan additional items against heuristics
- Scan inside archives
- Enable Advanced heuristics engine
- Action for potentially unwanted programs (PUP): `Do not detect`, `Detect and remove`, `Detect but do not remove`.
- Action for potentially unwanted modifications (PUM): `Do not detect`, `Detect and remove`, `Detect but do not remove`.
- Action for peer-to-peer software (P2P): `Do not detect`, `Detect and remove`, `Detect but do not remove`.

Updater Settings Tab

- Notify user when a program update is ready for installation - If checked, user is notified when a program update is ready for installation
- Proxy
  - Use proxy server to download updates - If checked, updates are downloading using proxy server.
    - ✓ Proxy server - Enter proxy server.
    - ✓ Port - Enter port.
  - Use authentication - If checked, you can enter Username and Password that will be used for authentication.

Endpoints tab

`Anti-Malware > Configuration > Alerts > Endpoints`

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

Note: The Machines > **Details** *(page 11)* > **Alert Profiles** tab displays the list of **alert profiles** *(page 21)* assigned to a selected machine.

Alerts

Anti-Malware > Configuration > Alerts

The **Alerts** page manages **Anti-Malware** 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 Anti-Malware > **Machines** *(page 5)* > **Alert Profiles**. Different types of machines may require different alert profiles. Alert profiles are visible to all VSA users.

Note: Alert profile *creation and configuration are shared* between both **Antivirus** and **Anti-Malware**. Alert profile *assignment is not shared*. You must assign the alert profile to each machine separately in both modules.

Reviewing Alarms Created by Anti-Malware Alerts

- Monitor > **Alarm Summary** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#1959.htm)*
- Monitor > Dashboard List > any **Alarm Summary Window** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#4112.htm)* within a dashlet
- Agent > Agent Logs > **Agent Log** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#354.htm)*
- The Agent > Agent Logs > **Monitor Action Log** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/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/9050000/index.asp#33845.htm)* > 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.

In This Section

Summary tab

Anti-Malware > Configuration > Alerts > New/Edit > Summary tab

General Tab

- **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

Anti-Malware > Configuration > Alerts > New/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 and Configuration Data

- **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** - 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 12)* 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 manage security product repair failed.
- **Client uninstall failed** - A managed security product uninstall failed.
- **Client license deactivated** - A managed security product license deactivated.

Actions tab

Anti-Malware > Configuration > Alerts > New/Edit > Actions tab

The **Actions** tab of an alert profile determines the actions taken in response to any of the **Alert Types** *(page 22)* 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** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#4119.htm)*.
- **Send Message to Notification Bar** - If checked and an alert condition is encountered, a notification is sent to the specified user's **Notification Bar** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#10634.htm)*.

Endpoints tab

Anti-Malware > Configuration > Alerts > New/Edit > Endpoints

The **Endpoints** tab lists all machines using the selected **Anti-Malware** profile.

Note: The Machines > **Details** *(page 11)* > **Alert Profiles** tab displays the list of **alert profiles** *(page 21)* assigned to a selected machine.

Actions

- Add - Adds a new machine to an alert. Select machines in appeared Choose Endpoints window.
- Deletes - Deletes selected machine.

Settings

Anti-Malware > Configuration > Settings

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

In This Section

Global Exclusions tab

Anti-Malware > Configuration > Settings > Global Exclusions

The **Global Exclusions** tab excludes objects from **Anti-Malware** monitoring. You can optionally apply these global exclusions by checking the **Include Global Settings** checkbox on the **Exclusions** *(page 19)* tab of the profile.

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

Exclusion Rules

- **New** - Adds entries to be excluded from scanning and protection, up to a limit of 256 exclusions. Wildcards are not supported.
  - Type - Select type from the drop-down: File, Folder, IPv4, Registry Key, Registry Value.
  - Path - Path must begin with a drive letter. Examples: `C:\Windows\file.exe` or `C:\Windows\folder`.
- **Edit** - Edits a selected exclusion rule.
- **Delete** - Deletes a selected exclusion rule.

Application Settings tab

Anti-Malware > Configuration > Settings > Global Exclusions

The **Application Settings** tab sets the privacy option for profiles. Profiles are public by default.

- **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.
- **Use LAN Updater** - If checked, the Agents LAN Cache settings will be used to set up a LAN Updater for updating Definition Files.

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.

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

- **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** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#4119.htm)*.
- **Send Message to Notification Bar** - If checked and an alert condition is encountered, a notification is sent to the specified user's **Notification Bar** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#10634.htm)*.

Chapter 4

Administration

In This Chapter

Application Logging

Anti-Malware Application Logging

The **Application Logging** page displays a log of **Anti-Malware** module activity by:

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

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

Index