Anti-Malware (Classic)

User Guide

Version R93

English

November 18, 2016

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

Anti-Malware (Classic) 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 (Classic) (KAM) provides Malwarebytes' Anti-Malware Pro endpoint security for managed machines. **Anti-Malware (Classic)** can be installed independently of **Endpoint Security** or **Antivirus (Classic)**. **Anti-Malware (Classic)** 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 (Classic) 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 XP, Vista, 7, 8 and 8.1 (32-bit and 64-bit).
- 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.
- No reboot required after install.
- Protection controls entire machine, beyond individual accounts.
- Supports exclusions of files, folders, registry keys and values, and IP4 addresses.
- Policy Management can manage the assignment of Anti-Malware (Classic) profiles.

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 **Anti-Malware (Classic)** endpoints—except for Malwarebytes Signature file updates—use LAN Cache automatically, if LAN Cache is already configured for those endpoints. No additional configuration in **Anti-Malware (Classic)** is required. See Agent > **LAN Cache** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/index.asp#9328.htm)* for more information.

Note: *See* **Anti-Malware (Classic) System Requirements** *(page 3).*

Functions	Description
Machines *(page 3)*	Installs and uninstalls Anti-Malware (Classic) software on selected machines and provides a detailed view of the Anti-Malware (Classic) status of any selected machine.

Dashboards *(page 10)*	Displays a dashboard view of the status of all machines installed with Anti-Malware (Classic).
Detections *(page 11)*	Displays virus threats you can take action on.
Profiles *(page 12)*	Manages Anti-Malware (Classic) profiles that are assigned to machine IDs.
Alerts *(page 15)*	Manages Anti-Malware (Classic) module alerts.

Anti-Malware (Classic) Module Minimum Requirements

Kaseya Server

- The Anti-Malware (Classic) R93 module requires VSA R93.

Requirements for Each Managed Workstation

- 800 MHZ processor.
- 2048 MB of RAM.
- 25 MB free disk space.
- Microsoft Windows XP SP3, Vista, 7, 8, 8.1, 10. Apple and Linux are not supported. Servers 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/9030000/reqs/index.asp#home.htm).*

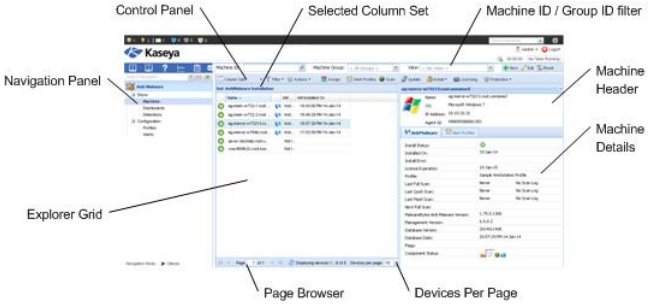
Machines

Anti-Malware (Classic) > Show > Manage Machines

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

Page Layout

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



- **Navigation Panel** - Used to navigate to pages within the **Anti-Malware (Classic)** 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 (Classic)** - Displays a summary of the **Anti-Malware (Classic)** status of a machine.
  - **Alert Profiles** - Lists the alert profiles assigned to a machine.

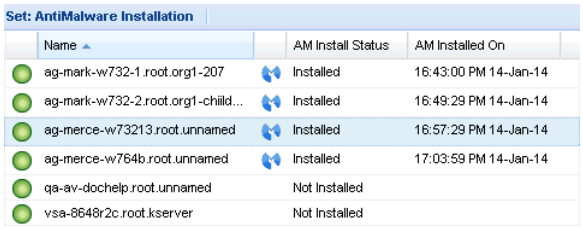
Explorer Grid

The **Explorer Grid** of the Machines page lists each machine currently installed with **Anti-Malware (Classic)** *and* included in the **machine ID / group ID filter** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/index.asp#209.htm)*.

Note: The only exception is when `Anti-Malware (Classic) Installation` is selected. In this case all machines included in the machine ID /group ID filter are displayed.

- The *set of columns* displayed is determined by the **Column Set** selection in the **Control Pane** *(page 5)*l. The currently selected column set displays in the bar just above the **Explorer Grid**.

  Note: See **Anti-Malware (Classic) Columns** *(page 7)* 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

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* **Anti-Malware (Classic) Columns** *(page 7)* for a description of each column available to display in *any* **Explorer Grid** column set.

- **Anti-Malware (Classic) Installation** - Displays **Anti-Malware (Classic)** installation columns in the **Explorer Grid** *for all agent machines*.
- **Anti-Malware (Classic) Status** - Displays status columns in the **Explorer Grid** for all agent machines *installed with an* **Anti-Malware (Classic)** *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 `Anti-Malware (Classic) Upgrade Recommended` filter helps you identify which machines are eligible for upgrading to the latest version. To upgrade, install over an existing installation of **Anti-Malware (Classic)**.

Actions

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

Assign

Assigns a **Anti-Malware (Classic)** configuration profile to selected machines. See **Profiles** *(page 12)* for more information.

Alert Profiles

Assigns or removes an alert profile for selected machines. The **Alert Profiles** tab on the **Details Panel** *(page 9)* displays all profiles assigned to a machine.

Scan

Schedules an **Anti-Malware (Classic)** 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 **Anti-Malware (Classic)** 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 (Classic)** 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 Anti-Malware (Classic)** - Installs or upgrades the **Anti-Malware (Classic)** client on selected machines.
  - **Profile Selection** - Workstations can be selected and installed at the same time. Workstations are assigned the selected workstation profile.
  - **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.
  - **Blocking Install Issues** - Lists issues that can prevent a successful installation on selected machines.
- **Uninstall Anti-Malware (Classic)** - Uninstalls the **Anti-Malware (Classic)** 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 Anti-Malware (Classic) Install** - Re-installs missing files on a previously installed **Anti-Malware (Classic)** client to repair it. The **Anti-Malware (Classic)** client must have been previously installed using **Anti-Malware (Classic)** for 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 Anti-Malware (Classic)** - Reestablishes a connection to a machine that was previously managed by **Anti-Malware (Classic)** but had the Kaseya agent removed, then re-installed. This includes reestablishing 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 multiple verifications evenly across a distribution window no later than the number of periods specified, to spread network traffic and server loading.
  - **Anti-Malware (Classic) Selection** - Selects the workstation profile that is applied.

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 (Classic)** license counts for workstations. **Anti-Malware (Classic)** license counts also display on the Administration > Manage > **License Manage** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/index.asp#2924.htm)* page.
  - `Purchased`
  - `Deployed` - Active license applied to a machine.
  - `Pending Install` - Scheduled for install, but install not yet complete.
  - `Full Available` - Purchased not applied or expired.
  - `Expiring in # Days` - Days remaining before all licenses expire.
  - `Expiry Date`

Protection

- **Get Status** - Returns the enable/disabled status of **Anti-Malware (Classic)** 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 (Classic)** - Re-enables **Anti-Malware (Classic)** protection on selected machines.
- **Temporarily Disable Anti-Malware (Classic)** - Disables **Anti-Malware (Classic)** protection on selected machines. Some software installations require **Anti-Malware (Classic)** software be disabled to complete the install.

Anti-Malware (Classic) 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 5)*.

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 5)* to modify a column set.

Anti-Malware (Classic)

- **AM Components** - Identifies the status of **Anti-Malware (Classic)** components installed on this machine.
- **AM Database Version** - The version of the **Anti-Malware (Classic)** definition database currently being used by this machine.
- **AM Expiration Date** - The date **Anti-Malware (Classic)** security is scheduled to expire.
- **AM Install Status** - `Not Installed`, `Script Scheduled`, `Installed`, `Installed (New AM)`
- **AM Installed On** - The date **Anti-Malware (Classic)** was installed.
- **AM Last Updated** - The date the **Anti-Malware (Classic)** definition database was last updated.
- **AM Profile** - The **Anti-Malware (Classic)** profile assigned to this machine.
- **AM Program Version** - The Malwarebytes version number of the **Anti-Malware (Classic)** client installed on this machine.
- **AM Service Version** - The version of the **Anti-Malware (Classic)** client.
- **AM Flags** - Possible flags include: `Definitions out of date`
- **AM Install Phase Icon** - If checked, **Anti-Malware (Classic)** is installed on the machine.
- **AM Pending Actions** - Icons representing install, assign, update and scan.

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 Quick View 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/9030000/index.asp#503.htm)*.

Scan

- **AM Last Flash Scan** - The date/time the last **Anti-Malware (Classic)** flash scan was performed. A flash scan analyzes memory and auto-run objects.
- **AM Last Full Scan** - The date/time the last **Anti-Malware (Classic)** full scan was performed. A full scan scans all files on the selected drives. A quick scan is recommended in most cases.
- **AM Last Quick Scan** - The date/time the last **Anti-Malware (Classic)** quick scan was performed. A quick scan uses fast scanning technology to scan systems for malicious software.

Status

- **Pending Actions** - Install, Assign, Update and Scan
- **Reboot Needed** - If `Yes`, a reboot is required.

Upgrade Ready

- **Available AM Client Version** - The Malwarebytes version number of the **Anti-Malware (Classic)** client available to upgrade on this machine.

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*. **Anti-Malware (Classic)** 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, **Anti-Malware (Classic)** security is installed. Select view log to view the log for the machine.
- **Installed On** - The date **Anti-Malware (Classic)** was installed.
- **Install Error** - If an install error occurs, displays a `View Log` link to the install log.
- **License Expiration** - The date **Anti-Malware (Classic)** security is scheduled to expire.
- **Profile** - The **Anti-Malware (Classic)** configuration profile assigned to this machine.
- **Last Full Scan** - The last date and time all files on selected drives were scanned using **Anti-Malware (Classic)**.
- **Last Quick Scan** - The last date and time a quick scan for malicious software was performed using **Anti-Malware (Classic)**.
- **Last Flash Scan** - The last date and time a flash scan analyzed memory and auto-run objects using **Anti-Malware (Classic)**.
- **Next Full Scan** - The next date and time an **Anti-Malware (Classic)** scan is scheduled to be performed.
- **Malwarebytes Anti-Malware Version** - The Malwarebytes version number of the **Anti-Malware (Classic)** client installed on this machine.
- **Management Version** - The Kaseya version of **Anti-Malware (Classic)** service installed.
- **Database Version** - The Malwarebytes version number of the **Anti-Malware (Classic)** definition database.
- **Database Date** - The date and time of the **Anti-Malware (Classic)** definition database currently being used by this machine.

- **Flags** - Possible flags include: `Definitions out of date`, `Out of Compliance`.

> **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 **Anti-Malware (Classic)** components installed on this machine.
  -  - Service is running or stopped.
  -  - Protection module is running or stopped.
  -  - File Execution Blocking is running or stopped.
  -  - Malicious website blocking is running or stopped.

Alert Profiles tab

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

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

Dashboards

Anti-Malware (Classic) > Show > Dashboards

The **Dashboards** page provides a dashboard view of the status of machines installed with **Anti-Malware (Classic)**. The dashboard statistics displayed depends on the **machine ID / group ID filter** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/index.asp#209.htm)* and machine groups the user is authorized to see using System > **Scopes** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/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.

Anti-Malware (Classic) Dashboard Parts

- **Anti-Malware (Classic) License Count** - A bar chart displays the number of **Anti-Malware (Classic)** licenses used and the number of machines pending an install.
- **Anti-Malware (Classic) License Summary** - A chart displays the number of machines that are `Available`, `Expired`, `In Use`, `Partials` and `Pending Install`.
- **Anti-Malware (Classic) Machines Needing Attention** - A bar chart displays the number of **Anti-Malware (Classic)** managed machines needing attention, by category. Categories include `No AM Installed`, `With Uncured Threats`, `Out of Date`, `Reboot Needed`, `Component Status`.
- **Anti-Malware (Classic) Machines with Detections** - A bar chart displays the number of detections.

- **Anti-Malware (Classic) Protection Status** - A pie chart displays percentage categories of machines with **Anti-Malware (Classic)** protection. Percentage categories include `Not Installed`, `Out of Date`, `Not Enabled`, and `Up to Date`.
- **Anti-Malware (Classic) 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 11)* page.

Detections

Anti-Malware (Classic) > Show > Manage Detections

The **Detections** page displays virus threats not automatically resolved by **Anti-Malware (Classic)**. 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/9030000/index.asp#209.htm)* and machine groups the user is authorized to see using System > **Scopes** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/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.
- **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 (Classic)** 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.

Profiles

Anti-Malware (Classic) > Configuration > Profiles

The **Profiles** page manages **Anti-Malware (Classic)** profiles. Each profile represents a different set of enabled or disabled **Anti-Malware (Classic)** options. Changes to a profile affect all machine IDs assigned that profile. A profile is assigned to machine IDs using Anti-Malware (Classic) > **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 - Workstations Only

Anti-Malware (Classic) profiles can only be assigned to workstations. A sample profile is provided.

Actions

- **New Profile** - Creates a new configuration profile. Profiles support Malwarebytes Anti-Malware versions 1.75.
- **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.

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 16)*
- **Protection tab** *(page 13)*
- **AM Scan tab** *(page 13)*
- **Update Options tab** *(page 14)*
- **Exclusions tab** *(page 14)*
- **Endpoints tab** *(page 15)*

Table Columns

- **Name** - Name of the profile.
- **Profile Type** - Anti-Malware
- **Machines Applied** - Number of machines using this profile.
- **Create by** - VSA user who created this profile.
- **Version** - KAM 1.75

Summary tab

Anti-Malware (Classic) > Configuration > Profiles > Summary tab

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

- **Profile Type** - **Anti-Malware (Classic)** workstation.
- **Profile Version -** `KAM 1.75`

Protection tab

Anti-Malware (Classic) > Configuration > Profiles > Protection

-  - **Start protection module with Windows** - 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.
  - **Show tooltip balloon when malicious website is blocked** - If checked, a tooltip balloon displays to the user when a malicious website is blocked.

AM Scan tab

Anti-Malware (Classic) > Configuration > Profiles > AM Scan

The **AM Scan** tab schedules recurring scans for a selected **Anti-Malware (Classic)** profile.

- **(Schedule Type)**
  - `Manually` - Scans of machines using this profile are only scheduled manually.
  - `By Schedule` - Schedules scans of machines using this profile by the specified number of time periods. Time is agent-based.
- **(Scan Type)**
  - `Full` - A full scan scans all files on the selected drives. A quick scan is recommended in most cases.
  - `Quick` - A quick scan uses fast scanning technology to scan systems for malicious software.
  - `Flash` - A flash scan analyzes memory and auto-run objects.
- **(Scan Interval)**
  - `<Period>/Run every/On Reboot` - Select the periods used to specify the interval between each **Anti-Malware (Classic)** scan. Alternatively, you can choose to scan only when a machine reboots.
- **Recover if missed after (hours)** - The number of hours to wait to attempt to run the scan again if the machine was unavailable to scan at the scheduled time.
- **Scan Run Time** - Agent time to start one time only or recurring scan.
- **Scan Run Date** - Agent date to start one time only or recurring 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.
- **Wake from sleep** - If checked, attempts to wake the computer from sleep to perform a scheduled scan.
- **Enable Advanced Heuristics engine** - If checked, adds another layer of protection to detect new and unknown malware.
- **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

Anti-Malware (Classic) > Configuration > Profiles > Update Options

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

- **Download and install program update if available** - If checked, program updates are downloaded and installed, if available.
- **(Schedule Type)**
  - `By Schedule` - Schedules updates of machines using this profile by the specified number of time periods. Time is agent-based.
  - `Manually` - Updates of machines using this profile are only scheduled manually. Update machines manually using the control panel of the **Machines** *(page 3)* page.
- **(Scan Interval)**
  - `<Period>/Run every/On Reboot` - Select the periods used to specify the interval between each **Anti-Malware (Classic)** updates. Alternatively, you can choose to update only when a machine reboots.
- **Recover if Missed after (hours)** - The number of hours to wait to attempt to run the update again if the machine was unavailable to update at the scheduled time.
- **Update Run Time** - Agent time to start one time only or recurring updates.
- **Update Run Date** - Agent date to start one time only or recurring updates.
- **Wake computer from sleep to perform task** - 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.
- **Use custom proxy server settings** - If checked, uses a proxy server to download updates.
  - **Address** - Enter a valid proxy server name or IP address.
  - **Port** - Enter a port number.
- **Specify Authentication Data** - If checked, proxy authentication is required.
  - **Username** - 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 address** - If checked, machines on the same network as the proxy server do not use the proxy server.

Exclusions tab

Anti-Malware (Classic) > Configuration > Profiles > Exclusions

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

Exclusion Rules

- **Add Exclusion** - Adds entries to be excluded from scanning and protection, up to a limit of 256 exclusions. Wildcards are not supported.
  - **File or folder** - File and folder paths must begin with a drive letter. Examples: `C:\Windows\file.exe` or `C:\Windows\folder`
  - **Registry key or value** - Registry keys and values must begin with a valid hive name, such as `HKCU`, `HKLM`, `HKCR`, `HKU`. Examples: `HKLM\Software\key` or `HKLM\Software\key|value`
  - **IP** - Examples: `111.222.33.444`
- **Delete** - Deletes a selected exclusion rule.

Endpoints tab

Anti-Malware (Classic) > Configuration > Alerts > Endpoints

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

Note: The Machines > **Details** *(page 9)* > **Alert Profiles** tab displays the list of **alert profiles** *(page 15)* assigned to a selected machine.

Alerts

Anti-Malware (Classic) > Configuration > Alerts

The **Alerts** page manages **Anti-Malware (Classic)** 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 (Classic) > **Machines** *(page 3)* > **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 (Classic)** or **Anti-Malware (Classic)** are visible and editable in both products. If a machine is assigned an alert profile using either **Antivirus (Classic)** or **Anti-Malware (Classic)**, the alert profile is assigned to both products on that machine.

Reviewing Alarms Created by Anti-Malware (Classic) Alerts

- Monitor > **Alarm Summary** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/index.asp#1959.htm)*
- Monitor > Dashboard List > any **Alarm Summary Window** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/index.asp#4112.htm)* within a dashlet
- Agent > Agent Logs > **Agent Log** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/index.asp#354.htm)*
- The Agent > Agent Logs > **Monitor Action Log** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/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/9030000/index.asp#33845.htm)* > Asset > Log Viewer > Alarm
- 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** *(page 12)*
- **Alert Types tab** *(page 16)*

- **Actions tab** *(page 16)*
- **Endpoints tab** *(page 17)*

Table Columns

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

Summary tab

Anti-Malware (Classic) > Configuration > Alerts > Summary tab

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

Alert Types tab

Anti-Malware (Classic) > Configuration > Alerts > Alert Types tab

Note: Setting an alert for KAM 6.5 also sets it for KAV 6.5.

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 11)* 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

Anti-Malware (Classic) > Configuration > Alerts > Actions tab

The **Actions** tab of an alert profile determines the actions taken in response to any of the **Alert Types** *(page 16)* 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 **Anti-Malware (Classic)** alerts using the Info Center > **Inbox** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/index.asp#4119.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 **Anti-Malware (Classic)** alerts using the **Notification Bar** *(http://help.kaseya.com/webhelp/EN/VSA/9030000/index.asp#10634.htm)*.

Endpoints tab

Anti-Malware (Classic) > Configuration > Profiles > Endpoints

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

Index