



Kaseya 2

Endpoint Security

User Guide

Version 2.1

July 19, 2011

About Kaseya

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

Contents

Security Overview	1
Dashboard	3
Security Status	4
Enable/Disable Resident Shield by Agent Procedure.....	6
Manual Update	7
Schedule Scan	10
View Threats	11
View Logs	13
Extend/Return	13
Notify.....	15
Install/Remove: Security.....	16
Define Profile	20
Assign Profile	26
Log Settings: Security	27
Exchange Status.....	28
Define Alarm Sets.....	29
Apply Alarm Sets.....	30
Security Reporting in VSA 5.x.....	33
Security Reporting in VSA 6.x.....	34
Index	35

Security Overview

Endpoint Security (KES) provides security protection for managed machines, using fully integrated anti-malware technology from AVG Technologies. The term **malware** encompasses viruses, spyware, adware and other types of unwanted programs. **Endpoint Security** automatically cleans or removes infected files and other threats such as trojans, worms and spyware. **Endpoint Security** continuously monitors the security status of all Windows servers, workstations and notebooks installed with security protection. Alarms can be triggered by security protection events and can include sending email notifications, running procedures, and creating job tickets.

Centrally managed security profiles are defined and deployed to machines using the VSA console interface. Changes to a security profile automatically update all machines using that profile. **Endpoint Security** comes with a pre-defined standard security profile and enables you to create customized security profiles.

All security protection events are logged within the system and available for executive summary and detailed management reporting. Once deployed, updates are handled automatically on a scheduled basis without the need for user interaction.

Anti-Virus Protection

Based on the security profile, **Endpoint Security** removes infected files or blocks access to them:

- **Scans the system registry** for suspicious entries, temporary internet files, tracking cookies, and other types of unwanted objects.
- **Detects computer viruses** by:
 - **Scanning** - Performs both on-access and on-demand scanning.
 - **Heuristic Analysis** - Dynamically emulates a scanned object's instructions within a virtual computing environment.
 - **Generic Detection** - Detects instructions characteristic of a virus or group of viruses.
 - **Known Virus Detection** - Searches for character strings characteristic of a virus.
- **Scans Email** - Checks incoming and outgoing email by using plug-ins designed for the most frequently used email programs. Once detected, viruses are cleaned or quarantined. Some email clients may support messages with text certifying that sent and received email has been scanned for viruses. In addition, for an increased level of security when working with email, an attachment filter can be set by defining undesirable or suspect files.
- **Memory-Resident Protection** - Scans files as they are copied, opened or saved. If a virus is discovered, file access is stopped and the virus is not allowed to activate itself. Memory resident protection is loaded into the memory of the computer during system startup and provides vital protection for the system areas of the computer.
- **On Demand Scans** - Scans can be run on-demand or scheduled to run periodically at convenient times.
- **Scans MS Exchange Servers** - Scans inbound and outbound email messages and mailbox folders on MS Exchange Servers against virus/spyware/malware threats and deletes them immediately before email recipients of the MS Exchange Server are infected.
- **Scans Websites and Downloads** - Scans websites and website links. Also scans files you download to your computer. Provides a safety rating for links returned by popular search engines.
- **ID Protection** - Prevents targeted theft of passwords, bank account details, credit card numbers, and other digital valuables using "behavioral analysis" to spot suspicious activity on a machine.

Anti-Spyware

Spyware is software that gathers information from a computer without the user's knowledge or consent. Some spyware applications may also be secretly installed and often contain advertisements, window pop-ups or different types of unpleasant software. Currently, the most common source of infection is websites with potentially dangerous content. Other methods of transmission include email

or transmission by worms and viruses. The most important protection against spyware is using a **memory resident shield**, such as the cutting edge **Endpoint Security** spyware component. A memory resident shield scans applications in the background as they run. **Endpoint Security** anti-spyware protection detects spyware, adware, DLL-trojans, keyloggers, malware hidden in data streams, archives, spyware entries in the Windows registry and other types of unwanted objects.

Note: See [System Requirements](#).

Endpoint Security Licensing

Each MSE KES seat license allows the Customer to install and use an MSE KES agent perpetually and also to receive Updates for a Subscription Term of 365 consecutive days. The update Subscription Term runs independently for each seat and begins upon the date of installation of the MSE KES agent on a machine and allows the Seat to receive the KES Updates released during the Subscription Term. All Updates released during the Subscription Term are also licensed on a perpetual basis; provided that once the Subscription Term terminates or is not renewed the right to receive new KES Updates terminates.

Issuing a new Seat License to a machine with an existing Subscription Term causes the Terms to merge and thereby adds 365 days to the time otherwise remaining on the seat’s Subscription Term. Any transfer of such a merged Term to a new machine will cause all remaining days for both previous seats to be transferred.

The appropriate KES seat license must be obtained for each machine and/or Exchange Mailbox protected. The Customer may only deploy MSE KES on a machine that has a valid VSA license. MSE KES licenses can be centrally managed using Kaseya’s Web User Interface.

Note: KES licenses are allocated to group IDs using [System > License Manager](#).

Functions	Description
Dashboard (page 3)	Provides a dashboard view of the status of machines installed with Endpoint Security.
Security Status (page 10)	Displays the current security status of machine IDs.
Manual Update (page 7)	Schedules updates of the latest version of security protection definition files.
Schedule Scan (page 10)	Schedules security protection scans of machine IDs.
View Threats (page 11)	Lists files that have been placed in quarantine due to a suspicious or confirmed threat.
View Logs (page 13)	Displays the security protection event log of machine IDs.
Extend/Return (page 13)	Extends the annual license count for selected machines IDs or returns annual licenses from selected machine IDs.
Notify (page 15)	Provides automatic notification of the expiration of Endpoint Security licenses.
Install/Remove (page 16)	Installs or removes security protection for machine IDs.
Define Profile (page 20)	Manages security profiles. Each security profile represents a different set of of enabled or disabled security options.
Assign Profile (page 26)	Assigns security profiles to machine IDs.
Log Settings (page 27)	Specifies the number of days to keep security protection log data.
Exchange Status (page 28)	Displays the status of email protection on MS Exchange servers that have KES installed on them.
Define Alarm Sets (page 29)	Defines sets of alarm conditions used to trigger alerts using the Apply Alarm Sets page.

Dashboard

Security > Dashboard

- Similar information is provided by [Info Center > Reports > Security](#).

The **Dashboard** page provides a dashboard view of the status of machines installed with **Endpoint Security**.

- [Endpoint Security Statistics](#)
- [License Status](#)
- [Top Machines with Threats](#)
- [Top Threats Discovered](#)

Note: The list of machine IDs displayed depends on the Machine ID / Group ID filter and machine groups the user is authorized to see using [System > User Security > Scopes](#).

Endpoint Security Statistics

The **Endpoint Security Statistics** section provides various statistics about the security status of endpoints and the status of security definitions.

- <N> Endpoints Need Reboot
- <N> Signature versions older than '62'
- <N> Endpoints with older version of **Endpoint Security**
- <N> Endpoints not having a scan completed this week
- <N> Endpoints currently running a scan
- <N> Endpoints with Resident Shield disabled

Click any of these hyperlinked statistics to see a tabbed dialog showing each member belonging to that statistic.

License Status

A pie chart displays the percentage of machines that have expired licenses or will have expired licenses in 30, 60, 90 or 91+ days. Click any slice of the pie chart or any label of the pie chart to display a list of individual machines belonging to that slice.

Top Machines with Threats

Lists the machines with the greatest number of current threats. The number of threats in the virus vault are also listed. Clicking a hyperlinked machine ID displays the threats belonging to that machine ID in the [View Threats](#) (page 11) page.

Top Threats Discovered

A pie chart displays which threats have been found on the greatest percentage of machines. Click any slice of the pie chart or any label of the pie chart to display a list of individual machines belonging to that slice in the [View Threats](#) page.

Security Status

Security > Security Status

- Similar information is provided by [Info Center > Reports > Security](#).

The **Security Status** page displays the current security status of each machine ID licensed to use **Endpoint Security**. The list of machine IDs displayed depends on the Machine ID / Group ID filter and machine groups the user is authorized to see using [System > User Security > Scopes](#). To display on this page, machine IDs must have the **Endpoint Security** client software installed on the managed machine using the [Security > Install/Remove \(page 16\)](#) page.

Indicators include resident shield protection, mail protection, the number of unresolved threats detected, the number of threats in the virus vault and the version of security protection installed on each machine ID.

This page provides the following actions:

- **Enable Resident Shield** - Click to enable resident memory anti-malware protection on selected machines IDs.
- **Disable Resident Shield** - Click to disable resident memory anti-malware protection on selected machines IDs.

Note: In some cases, security protection must be disabled to install or configure software on a managed machine.

Note: You can also [Enable/Disable Resident Shield by Agent Procedure \(page 6\)](#).

- **Enable Email** - Click to enable email protection on selected machines IDs.
- **Disable Email** - Click to disable email protection on selected machines IDs.
- **Empty Vault** - Click to empty the virus vault of all quarantined malware IDs.
- **Reboot Now** - Reboots selected machines IDs. Some security updates require a reboot to install the update. If a reboot is pending, a reboot icon displays alongside the pre-update version number and the machine is still protected.

Current Available Signature Version









The latest version of security protection available. You can update one or more machine IDs with the **Current Available Version** using [Security > Manual Updates \(page 30\)](#).

Current Installer Version

The version number of the AVG installer to be used on new installations.

Check-in 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

Note: Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > **Control Machine** page displays a legend of the specific icons your VSA system is using.

(Select All Checkbox)

Click this checkbox to select all rows in the paging area. If checked, click this checkbox to unselect all rows in the paging area.

Machine.Group ID














The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.




Profile Name

The security profile assigned to the machine ID.

Status

The current state of security protection for a machine ID is indicated by the set of status icons displayed in the **Status** column. Possible status icons include:

	Resident Shield On
	Resident Shield Off
	Resident Shield Partial
	Resident Shield Enable/Disable Pending
	Email Scanner On
	Email Scanner Off
	Email Scanner Partial
	Email Scanner Enable/Disable Pending
	Link Scanner On
	Link Scanner Off
	Link Scanner Partial
	Link Scanner Enable/Disable Pending
	Web Shield On

	Web Shield Off
	Web Shield Partial
	Web Shield Enable/Disable Pending

Threats

The number of unhealed threats detected on the machine ID. These are current threats that need user attention. You can click the hyperlinked number in any row to display these threats in the **Current Threats** tab of the **View Threats** (*page 11*) page.

Virus Vault

The number of threats stored in the virus vault of the machine ID. These items are safely quarantined and will be automatically deleted, if profile settings apply. You can click the hyperlinked number in any row to display these threats in the **Virus Vault** tab of the **View Threats** (*page 11*) > page.

Version

The version of security protection currently used by this machine ID.

For example: 8.5.322 270.12.6/2084

- 8.5.322 - The version of AVG program installed.
- 270.12.6/2084 - The full virus *database* version. 270.12.6 represents the *definition* version and 2084 is the *signature* version. Displays in red text if the *signature* version is older than the last 5 *signature* versions available or if the *definition* version is older than the last 2 *definition* versions available and the agent is active.

Note: If a machine ID's version is outdated you can update machine IDs manually using [Security > Manual Update](#) (*page 7*).

Note: Some security updates require a reboot to install the update. If a reboot is pending, a reboot icon displays alongside the pre-update version number and the machine is still protected.

Enable/Disable Resident Shield by Agent Procedure

You can disable/enable **Resident Shield** using the following **Execute Shell Command** in an agent procedure. In the agent working directory, run:

```
C:\kworking\kes>KasAVCmd -setFileMonitorEnable 0 ;disables Resident Shield
C:\kworking\kes>KasAVCmd -setFileMonitorEnable 1 ;enables Resident Shield
```

```
Script Name: KES_Enable Resident Shield
Script Description: Enables Resident Shield temporarily (until next scan or
reboot...unless it is enabled by default and is being re-enabled after being
temporarily disabled)
IF True
THEN
  Get Variable
    Parameter 1 : 10
    Parameter 2 :
    Parameter 3 : agenttemp
      OS Type : 0
  Execute File
    Parameter 1 : #agenttemp#\kes\KasAVCmd.exe
    Parameter 2 : -setFileMonitorEnable 1
    Parameter 3 : 3
      OS Type : 0
ELSE
```

```
Script Name: KES_Disable Resident Shield
Script Description: Disables Resident Shield temporarily (until next scan or
reboot)
IF True
THEN
  Get Variable
    Parameter 1 : 10
    Parameter 2 :
    Parameter 3 : agenttemp
      OS Type : 0
  Execute File
    Parameter 1 : #agenttemp#\kes\KasAVCmd.exe
    Parameter 2 : -setFileMonitorEnable 0
    Parameter 3 : 3
      OS Type : 0
ELSE
```

Manual Update


Security > Manual Update

The **Manual Updates** page controls the updating of machine IDs licensed to use **Endpoint Security** with the latest version of security protection available. *Updates are scheduled automatically by default.* You can disable and re-enable automatic updating by machine. Typically this function is only used to review the update status of agents or to force an immediate update check if needed.

The list of machine IDs you can select depends on the machine ID / group ID filter. To display on this page, machine IDs must have the **Endpoint Security** client software installed on the managed machine using the Security > **Install/Remove** (page 16) page.

This page provides the following actions:

- **Update** - Click to schedule a virus definition update on selected machine IDs using the update options previously selected.

- **Cancel Update** - Click to clear a scheduled update.
- **Enable Automatic Updates** - Enables virus definition updates.
- **Disable Automatic Updates** - Disables virus definition updates. This prevents virus definition updates from slowing down the network during peak working hours. In a future release you will be able to schedule when to update virus definitions. If automatic updates are disabled, then a red-cross icon  displays in the **Scheduled Time** column, even if a manual update is scheduled.

Current Available Version

The latest version of security protection available. Check the version column on this page to determine if any machine IDs are missing the latest version of security protection or the latest **Endpoint Security** client software available.

Current KES Client Version

The latest KES client software available.

Update from KServer (Override file source)

If checked, updates are downloaded from the KServer. If blank, updates are downloaded using the method specified in Patch Management > File Source.

Immediate

Check the **Immediate** box to begin the update as soon as **Update** is clicked.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Stagger by









You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...

Skip if Machine Offline

Check to perform this task only at the scheduled time, within a 15 minute window. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.

Check-in 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

Note: Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

(Select All Checkbox)

Click this checkbox to select all rows in the paging area. If checked, click this checkbox to unselect all rows in the paging area.

Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Source

If a file source is defined using Patch Management > File Source, then updates are sourced from this location. Otherwise, updates are sourced from the internet.

If the option **Download from Internet if machine is unable to connect to the file server** is selected in Patch Management>File Source:

- During a **Endpoint Security** v2.x endpoint install, if the files source is down or credentials invalid, the installer is downloaded from the Kserver and completes the endpoint install.
- During a **Endpoint Security** v2.x manual update, if the files source is down or credentials invalid, the update is downloaded from the internet.

In both cases above, the **View Logs** (*page 13*) page displays an error message stating why the file source failed and that it is trying to download from the internet.

Last Update

This timestamp shows when a machine ID was last updated. When this date changes, a new update is available to use.

Version


The version of security protection currently used by this machine ID.

For example: 8.5.322 270.12.6/2084

- 8.5.322 - The version of AVG program installed.
- 270.12.6/2084 - The full virus *database* version. 270.12.6 represents the *definition* version and 2084 is the *signature* version. Displays in red text if the *signature* version is older than the last 5 *signature* versions available or if the *definition* version is older than the last 2 *definition* versions available and the agent is active.
- [KES 2.1.0.87] - The version of **Endpoint Security** client software.

Scheduled Time

Timestamp showing the next scheduled update, if one is scheduled either manually or automatically. For a selected machine:

- If *automatic updates are enabled* for a selected machine and KES detects an AVG update, a time stamp displays. When multiple machines are scheduled, the timestamps will differ because automatic updates uses a staggered schedule.
- If *automatic updates are enabled* but no AVG update is detected, the table cell is blank, unless a manual update is also scheduled.
- If *automatic updates are disabled*, then a red-cross icon  displays, even if a manual update is scheduled.
- If a *manual update is scheduled*, a time stamp displays.

Schedule Scan

Security > Schedule Scan

The **Schedule Scan** page schedules security protection scans of selected machine IDs licensed to use **Endpoint Security**. The list of machine IDs you can select depends on the machine ID / group ID filter. To display on this page, machine IDs must have the **Endpoint Security** client software installed on the managed machine using the Security > **Install/Remove** (page 16) page.

This page provides the following actions:

- **Scan** - Click to schedule a scan of selected machine IDs using the scan options previously selected.
- **Cancel** - Click to clear a scheduled scan.

Immediate

Check the **Immediate** box to begin the scan as soon as **Scan** is clicked.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...

Skip if Machine Offline









Check to perform this task only at the scheduled time, within a 15 minute window. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.

Every N Periods

Check the box to make this task a recurring task. Enter the number of periods to wait before running this task again.

Check-in 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

Note: Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

(Select All Checkbox)

Click this checkbox to select all rows in the paging area. If checked, click this checkbox to unselect all rows in the paging area.


Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Last Scan

This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.

Next Scan / Schedule

This timestamp shows the next scheduled scan. Overdue date/time stamps display as **red text with yellow highlight**. A green  checkmark indicates the scan is recurring.

View Threats

Security > View Threats

- Similar information is provided by Info Center > Reports > Security.

The **View Threats** page displays threats you can take action on. Threats are grouped by their status on two different tabs:

- **Current Threats** - Lists discovered threats on machines that could not be automatically healed. Each unhealed threat remains unchanged on the machine, requiring user action. Deleting a threat on the **Current Threats** tab deletes the file immediately, without moving the file to the **Virus Vault**.

Note: When a machine is scanned, all of its current threats are cleared out and marked as resolved. If a threat continues to exist, it is rediscovered and added back to the current threats list.

- **Virus Vault** - Threats are discovered by scan or resident shield. Healing the threat replaces the original file with a healed copy. The original, unhealed file is moved to a hidden partition on the computer hard drive called the **Virus Vault**. In effect, the **Virus Vault** acts as a kind of "recycle bin" for threats, allowing you to recover them before deleting them permanently from machines.

Healing

Healing involves the following steps:

1. An attempt is made to clean the file.
2. If that fails, an attempt is made to move the file to the **Virus Vault**.
3. If that fails, an attempt is made to delete the file.
4. If that fails, the file remains unchanged on the machine and is listed in the **Current Threats** tab of the **View Threats** page.

MS Exchange Server Threats

Any malware detected by MS Exchange Server email protection is immediately deleted from the MS Exchange Server and displays *only* on the **Virus Vault** tab.

Current Threats

The **Current Threats** tab provides you with the following actions:

- **Heal** - Attempts to heal a file without deleting it. Healed threats are removed from the **Current Threats** tab and display in the **Virus Vault** tab.
- **Delete** - Attempts to delete a file. Deleted threats are deleted from the computer immediately.

Note: If both healing and deletion fail, it may mean the file is open. Kill any processes keeping the file open and try to delete the file again.

- **Remove from this List** - Removes the threat from the **View Threats** page without performing any other action.
- **Cancel Pending Operation** - Cancels any of the other actions, if they have not yet been completed.
- **Add to PUP Exclusion List** - A threat is identified as a potential unwanted program, or PUP, by displaying a (P) next to the name of the threat on the **View Threats** page. PUP threats can be added to the exclusion list for the profile assigned to the machine they were found on. Exclusion means the file is no longer scanned as a potential threat on *all* machines assigned this profile. Only perform this action if you're certain the file is safe to use. The entire PUP Exclusion List is maintained using the **Define Profile** (page 20) > PUP Exclusions tab.

Note: Non-PUP threats cannot be added to the PUP Exclusion List.

Virus Vault

The **Virus Vault** tab provides you with the following actions:

- **Restore** - Restores the original file identified as a threat. Only perform this action if you're certain the file is safe to use.
- **Delete** - Deletes the original file identified as a threat from the **Virus Vault**.

Note: You cannot recover a file deleted from the **Virus Vault**.

- **Remove from this List** - Removes the threat from the **View Threats** page without performing any other action.
- **Cancel Pending Operation** - Cancels any of the other actions, if they have not yet been completed.
- **Add to PUP Exclusion List** - A threat is identified as a potential unwanted program, or PUP, by displaying a (P) next to the name of the threat on the **View Threats** page. PUP threats can be added to the exclusion list for the profile assigned to the machine they were found on. Exclusion means the file is no longer scanned as a potential threat on *all* machines assigned this profile. Only perform this action if you're certain the file is safe to use. The entire PUP Exclusion List is maintained using the **Define Profile** (page 20) > PUP Exclusions tab.

Note: Non-PUP threats cannot be added to the PUP Exclusion List.

Apply Filter / Reset Filter

Click **Apply Filter** to filter the rows displayed by the text entered in the **Machine.Group**, **Threat Path** or **Threat Name** fields. **Time** filtering and **Action** sorting occurs immediately. Click **Reset Filter** to display all rows of data.

Filter Fields

Filter the display of threats using text fields, a date range and/or drop-down lists. Include an asterisk (*) wildcard with the text you enter to match multiple records.

- **Machine.Group** - Filter by the machine ID.group ID of the managed machines reporting threats.
- **Threat Path** - Filter by pathname location of files on managed machines with reported threats.
- **Time** - Filter by a range of dates and times the threats were *last* detected. **Time** filtering occurs immediately.
- **Threat Name** - Filter by the name of the threat, as designated by the anti-malware definitions used to detect a threat.

- **Category** - Filter by the type of threat reported. Select **All OFF** or **All ON** to enable or disable all categories.
- **Action** - Filter by pending or completed actions taken against view threat records. Select **All OFF** or **All ON** to enable or disable actions. Action sorting occurs immediately.

View Logs

Security > View Logs

- Similar information is provided by [Info Center > Reports > Security](#).

The **View Logs** page displays the security protection event log of each machine ID licensed to use **Endpoint Security**. The list of machine IDs displayed depends on the Machine ID / Group ID filter and machine groups the user is authorized to see using [System > User Security > Scopes](#). To display on this page, machine IDs must have the **Endpoint Security** client software installed on the managed machine using the [Security > Install/Remove](#) (page 16) page.

Click a machine ID.group ID to display an event log. Each event displays the **Time**, an event **Code**, and in most cases a **Message** containing additional information. Security protection event codes describe one of three types of log entry:

- Errors
- Events
- Commands

Apply Filter / Reset Filter

Click **Apply Filter** to filter the rows by the date range entered in the **Time** fields and/or the text entered in the **Message** field. Click **Reset Filter** to display all rows of data.

Filter Fields

Filter the display of threats using text fields, a date range and/or drop-down lists. Include an asterisk (*) wildcard with the text you enter to match multiple records. Paging rows can be sorted by clicking column heading links.

- **Time, Min, Max** - Filter by a range of dates and times.
- **Code** - Filter by the category of log event reported. Select **All OFF** or **All ON** to enable or disable all categories.
- **Message** - Filter by message text.

Extend/Return

Security > Extend/Return

The **Extend/Return** page extends the annual license count for selected machines IDs or returns annual licenses from selected machine IDs. A annual license can be returned from one machine ID and be applied to another machine ID. Each machine ID can be allocated multiple years of security protection. **Endpoint Security** licenses are allocated to group IDs using [System > License Manager](#).

Note: See [KES Licensing in the Security Overview](#) (page ii) topic.

The list of machine IDs you can select depends on the machine ID / group ID filter. To display on this page, machine IDs must have the **Endpoint Security** client software installed on the managed machine

using the Security > [Install/Remove](#) (page 16) page.

The page provides you with the following actions:

- **Extend** - Extends the annual license count for selected machines IDs.
- **Return** - Returns annual licenses from selected machine IDs.
- **Auto Extend** - Enables automatic allocation of a new license the day the old license expires for selected machine IDs. Only full licenses are allocated using **Auto Extend**. If no additional licenses exist, allocation fails and security protection expires for the endpoint. Enabled by default. This option only displays for master role users.
- **Remove Auto Extend** - Disables auto extend for selected machine IDs. This option only displays for master role users.

Licenses Used

Displays the number of annual **Endpoint Security** licenses used, returnable and partial. These counts are not affected by the machine ID.group ID filter.

- **Used** - A license is used if it has been assigned at least once to any machine ID. The used license count includes all returnable, partial and expired licenses.
- **Returnable** - The total number of returnable licenses available.
- **Partial** - The total number of partially used licenses available. Partially consumed licenses are made available when **Endpoint Security** is uninstalled from a machine ID.

Note: The expiration date for partial licenses are still in effect and are consumed even if they are no longer assigned to any machine. For this reason partial licenses, if available, are always assigned first to any machine ID requiring a **Endpoint Security** license.

Show only licences expiring within 30 days

Limits the display of licenses in the paging area to those expiring within 30 days.

(Select All Checkbox)

Click this checkbox to select all rows in the paging area. If checked, click this checkbox to unselect all rows in the paging area.

Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Returnable

The number of annual licenses returnable from a machine ID. A machine ID with only one annual license cannot return any additional annual licenses.

Expires On

The date a machine ID's security protection expires, based on the number of annual licenses it has.

Auto Extend

If checked, auto extend is enabled for this machine ID.

At Limit

If the maximum number of annual licenses available to a group ID are being used, then each licensed machine ID in that group ID displays a **Yes** in the **At Limit** column. This alerts the user that more annual licenses may be required for that group ID. **Endpoint Security** licenses are allocated to group IDs using System > License Manager.

Notify

Security > Notify

The **Notify** page provides automatic notification of the expiration of **Endpoint Security** licenses. Customers, VSA users and machine users can be notified a specified number of days before **Endpoint Security** licenses expire. **Endpoint Security** licenses are allocated to group IDs using System > License Manager.

Note: See [KES Licensing in the Security Overview \(page ii\)](#) topic.

The list of machine IDs you can select depends on the machine ID / group ID filter. To display on this page, machine IDs must have the **Endpoint Security** client software installed on the managed machine using the Security > [Install/Remove \(page 16\)](#) page.

Send notification when license will expire in N days

Enter the number of days before the expiration date of an **Endpoint Security** license to notify customers, users and users.

Email Recipients (Comma separate multiple addresses)

Specify email addresses to send notification messages. Multiple email addresses must be separated by commas.

Apply

Click **Apply** to apply parameters to selected machine IDs. Confirm the parameters have been applied correctly in the machine ID list.

Clear









Click **Clear** to remove all parameter settings from selected machine IDs.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in 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

Note: Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > [Control Machine](#) page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Days

Shows the number of days before the license expiration date that notification will be sent.

Email Address List

Lists the email addresses notifications will be sent to.

Notify

If checked, email recipients will be forewarned that this machine ID's security license is about to expire. If blank, notification will not be sent.

Install/Remove: Security

Security > Install/Remove

The [Install/Remove](#) page installs or removes security protection for selected machine IDs. The list of machine IDs displayed depends on the Machine ID / Group ID filter and machine groups the user is authorized to see using System > User Security > Scopes. Installation requires a reboot of the managed machine.

[Endpoint Security](#) licenses are allocated to group IDs using System > License Manager.

Customizing Warnings about Application Conflicts

Kaseya maintains a list of standard applications that conflict with the [Endpoint Security](#) client. You can ensure you are warned about *additional* applications that conflict with the [Endpoint Security](#) client by listing them in a file on the KServer. The typical KServer install location is:

```
C:\Kaseya\WebPage\AntivirusTab\SeedData\UserConflictExes.txt
```

UserConflictExes.txt is a comma separated list of user specified [Endpoint Security](#) conflicting programs, one entry per line. Line entries should be formatted as follows:

```
example.exe, description of example.exe, reason for exclusion, excluded by which tech  
example2.exe, another description, reason, who excluded example2.exe
```

Use // at the beginning of any line to add comments.

The warning is displayed in the [Install Status](#) column of the [Install/Remove](#) page. The warning also displays if the conflicting application is installed *after* the [Endpoint Security](#) client is installed and a latest audit is performed. A [Endpoint Security](#) application conflict log entry is generated if the [Endpoint Security](#) client is installed despite the existence of a conflicting application.

Installing KES on Servers

Installing the following options on *servers* is not recommended.

- Options In [Define Profile](#) (page 20)
 - Email Scanner
- Options In [Installation Options](#) in [Install/Remove](#)
 - Web Shield
 - Link Scanner
 - Identity Protection
 - AVG Firewall

Action Buttons

This page provides the following actions:

- **Install** - Install **Endpoint Security** on selected machine IDs.

Warning: Uninstall all anti-virus/spyware/malware software on the managed machine before installing **Endpoint Security** client software.

- **Verify Install** - Displays only in Kaseya 2. Updates 5.x KES clients to K2 KES clients. Can also be used to install a K2 KES client when a standalone version of AVG is already installed on a managed machine.
- **Remove** - Remove **Endpoint Security** on selected machine IDs.
- **Cancel Pending Operation** - Cancel either of the first two actions, if they have not yet been completed.
- **Edit User Prompts** - Edit the warning prompt displayed to users, if a warning prompt is displayed. You can also specify the number of minutes the user is allowed to postpone installation. This option only displays for master role users.
- **Reboot Now** - Reboots the selected computer. Periodically AVG releases an update that requires a reboot. *Reboot Required* displays in the **Version** column.
- **Installation Options** - Configure the following installation options. These options apply to any installation you subsequently perform. Installation options are defined *by VSA user*.

Note: After the **Endpoint Security** client is installed on a machine ID, the installation options applied to that machine ID can be viewed by clicking the green check mark in the **Install Status** column.

Install Options

- **User Name** - If checked, enter a name associated with this install of **Endpoint Security**.
- **Company Name** - If checked, enter the name of the company associated with this install of **Endpoint Security**.
- **Target Directory** - If checked, enter a target directory. If blank, the default install directory is used.
- **Kill all running applications that prevent installation** - If checked, stops all running applications that might prevent successful installation.
- **Disable Windows Defender** - Running Windows Defender significantly degrades the performance of **Endpoint Security** and should be disabled by default using this option.
- **Reboot the computer after installation if needed**
 - If checked, AVG reboots the computer after installation. Kaseya does not control this event. While the endpoint reboots, the **Install Status** column may display a *Verifying Installation* message. Once the endpoint checks-in again, the installation completes and the **Install Status** column displays a green checkmark.
 - If blank, Kaseya controls the reboot. The **Install Status** column displays a **Reboot Required** button. The user can click the button to reboot the endpoint. Once the endpoint checks-in again, the installation completes and the **Install Status** column displays a green checkmark.
- **Enable end user directory scans** - Adds a right-click option to Windows Explorer, enabling the user to scan an individual file or directory immediately.
- **Hide AVG system tray icon** - If checked, hides the AVG icon in the system tray. If unchecked, the AVG icon displays only after AVG is installed and the machine rebooted.

Note: AVG changes made by the user locally using the AVG UI are reset each time the machine is restarted and when the profile is re-applied.

Script Options

- **Script to run before install** - Select an agent procedure.

- **Script to run after install** - Select an agent procedure.

Components

- **Link Scanner** - Blocks dangerous websites and checks links returned by the most popular search engines. Does not install to browsers running on Windows Server O/S.
 - **Active Safe Search** - Scans a link displayed in a web page, before you click it.
 - **Search-Shield** - Identifies the safety rating for a search link listed in Google, Yahoo and MSN search lists.
- **Web-Shield** - Scans downloaded files and files exchanged using instant messaging.
- **MS Office 2000 - 2007 Add-in** - Installs the AVG scanning plugin for Microsoft Office, versions 2000 through 2007.
- **Email Scanner** - If checked, installation detects the default email client on a machine and automatically installs the respective email scanning plug-in.
- **ID Protection** - If checked, AVG's Identity Protection option is enabled. Prevents targeted theft of passwords, bank account details, credit card numbers, and other digital valuables using "behavioral analysis" to spot suspicious activity on a machine.
- **Firewall (Not managed by Kaseya)** - If checked, AVG's firewall option is enabled. Blocks unauthorized access while permitting authorized communications. *The Endpoint Security client cannot be used to maintain the blacklists and whitelists required by this option.*
- **Exchange Server Plug-in (Setting ignored on non-Exchange machines)** - If checked, installs **Endpoint Security** email protection to MS Exchange Servers. This setting is ignored when the **Endpoint Security** client is installed to a non-MS Exchange Server machine.

Immediate

Check the **Immediate** box to begin the install as soon as **Install** is clicked.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...

Skip if Machine Offline

Check to perform this task only at the scheduled time, within a 15 minute window. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.

Applied Licenses

Displays the number of annual **Endpoint Security** licenses applied to machines.

License Pool

Displays the number of additional licenses available: partially-used **Endpoint Security** licenses and never-used **Endpoint Security** licenses. Partially-used license are always consumed first.

Install from KServer (override file source)

If checked, installs are downloaded from the KServer. If blank, installs are downloaded using the method specified in Patch Management > File Source.

Select Profile

Selects the security profile to assign a machine ID when security protection is installed.

Prompt user before install / Force install without warning user

Installation requires a reboot of the managed machine. If **Prompt user before install** is selected, the user is given the option of postponing the installation for a specified number of minutes. Otherwise **Force install without warning user** causes the software to be installed at the scheduled time without warning the user.









Note: Click [Edit User Prompts](#) to specify the number of minutes the user is allowed to postpone the installation.

Auto Refresh

Selecting this checkbox automatically updates the paging area every five seconds. This checkbox is automatically selected and activated whenever **Install** is clicked.

Check-in 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

Note: Different icon images display when this add-on module is installed in a 5.x VSA. The [Remote Control > Control Machine](#) page displays a legend of the specific icons your VSA system is using.

(Select All Checkbox)

Click this checkbox to select all rows in the paging area. If checked, click this checkbox to unselect all rows in the paging area.

Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Install Status

If checked, **Endpoint Security** client software is installed on the machine ID. If the agent software is earlier than 4.7.1, the message `Requires Agent Update` displays. If blank, **Endpoint Security** client software is *not* installed on the machine ID.

Note: After the **Endpoint Security** client is installed on a machine ID, the installation options applied to that machine ID can be viewed by clicking the green check mark in the **Install Status** column.

Install Source

If a file source is defined using Patch Management > File Source, then installs are sourced from this location. Otherwise, installs are sourced from the internet.

If the option **Download from Internet if machine is unable to connect to the file server** is selected in Patch Management>File Source:

- During a **Endpoint Security** v2.x endpoint install, if the files source is down or credentials invalid, the installer is downloaded from the Kserver and completes the endpoint install.
- During a **Endpoint Security** v2.x manual update, if the files source is down or credentials invalid, the update is downloaded from the internet.

In both cases above, the **View Logs** (page 13) page displays an error message stating why the file source failed and that it is trying to download from the internet.

Installed On

The date **Endpoint Security** client software was installed on the machine ID.

Version

The version of security protection currently used by this machine ID.

For example: 8.5.322 270.12.6/2084

- 8.5.322 - The version of AVG program installed.
- 270.12.6/2084 - The full virus *database* version. 270.12.6 represents the *definition* version and 2084 is the *signature* version. Displays in red text if the *signature* version is older than the last 5 *signature* versions available or if the *definition* version is older than the last 2 *definition* versions available and the agent is active.
- [KES 2.1.0.87] - The version of **Endpoint Security** client software.

Define Profile

Security > Define Profile

The **Define Profile** page manages security profiles. Each security profile represents a different set of enabled or disabled security options. Changes to a security profile affect all machine IDs assigned that security profile. A security profile is assigned to machine IDs using Security > **Assign Profile** (page 26). Typically different types of machines or networks require different security profiles. A sample profile is provided for you. You can't change the sample profile, but you can save it under a new name and make changes to the copy.

This page provides you with the following actions:

- **Save** - Saves changes to a security profile.
- **Save As** - Creates a new security profile by saving it using a different name.
- **Delete** - Deletes an existing security profile.
- **Share** - Shares a private security profile. Other users cannot see private security profiles. Sharing a private security profile makes it a public security profile. Share rights are assigned *by object*. There are three sharing checkbox options. The first two checkboxes are *mutually exclusive* and determine what share rights are assigned. If neither of the first two checkboxes are checked, the shared object can only be seen by the users given share access, but the object cannot be used nor edited. The **Shared** and **Not Shared** list boxes and the third checkbox determine who can see the object.
 - **Allow other administrators to modify** - If checked, share rights to the object includes being able to use it, view its details and edit it.
 - **Other administrators may use but may not view or edit** - If checked, share rights to the object only allows using it.
 - **Make public (seen by all administrators)** - If checked, ensures that *all* current and future VSA users can see the object. If blank, only selected user roles and users can see the shared

object. If blank, and new users or user roles are added later, you have to return to this dialog to enable them to see the specific object.

- **Take Ownership** - Takes ownership of any public security profile. This option only displays for master role users.

To Define or Maintain a Security Profile

1. Select a security profile from the **Select Profile** drop-down list.
2. Set options on security profile tabs:
 - **General**
 - **Resident Shield**
 - **Email Scanner**
 - **Full Scan**
 - **Exchange**
 - **Exclude Dirs**
 - **Exclude PUPs**
 - **Updates**
3. Click the **Save** or **Save As** button to save the security profile.

General

Virus Vault

Limit Size of the Vault - If checked, limits the size of the vault as specified using the following options:

- **Maximum Size of the Vault: <N>% of Local Disk** - Enter the maximum percentage of disk space to allocate for the storage of quarantined threats.
- **Minimum Available Space to Remain on Local Disk** - Enter the minimum number of megabytes to allocate on the disk to the storage of quarantined threats.

Automatic File Deletion - If checked, deletes files automatically as specified by the following options:

- **Delete Files Older than <N> Days** - Enter the number of days to store quarantined threats before they are automatically deleted.
- **Maximum Number of files to Store** - Enter the maximum number of quarantined threats to store.

System Tray Notifications

Display system tray notifications - If checked, the following system tray notifications can be optionally enabled. All notification messages display on the managed machine next to the system tray.

Display tray notifications about update - If checked, displays a notification message that the **Endpoint Security** software is being updated.

Display tray notifications about scanning - If checked, displays a notification message that the machine is being scanned.

Display Resident Shield related tray notifications (automatic action) - If checked, displays a notification message that Resident Shield has taken action against a threat.

Display components state change notification - If checked, displays a notification message that the state of one of the **Endpoint Security** components has changed.

Display Email Scanner related notifications - If checked, displays a notification message that email scanning has taken action against an email threat.

Agent Icon Menu

Display option to Enable/Disable Resident Shield in Agent Icon Menu - If checked:

- **Enable Security** and **Cancel Scan** options display in the agent task menu of the managed machine.
- The user can click the **Enable Security** option on the agent menu to turn security protection on or off.
- The user can click the **Cancel Scan** option on the agent menu to cancel an ongoing security protection scan.

Note: The user can also enable/disable security protection remotely using **Security > Security Status** (page 4).

Resident Shield

Resident shield is a memory-resident feature.

Enable Resident Shield - If checked, the following types of files are scanned as they are copied, opened or saved. If blank, no other **Resident Shield** options are evaluated.

Note: You can also **Enable/Disable Resident Shield by Agent Procedure** (page 6).

File Types

Scan all files - If selected, all files on the managed machine are scanned.

Scan Infectible files and Selected Document Types - If selected, specifies the *additional* file extensions of programs and documents to include or exclude using the following options:

- **Exclude files with the following extensions from the scan** - Specifies the file extensions of programs and documents to exclude from a scan. Excluded extensions have precedence over included extensions. Enter each extension separated by a semi-colon (;) character.
- **Always scan files with the following extensions** - Specifies the file extensions of programs and documents to include in a scan. Enter each extension separated by a semi-colon (;) character. Resident Shield scans the following file extensions without you having to specify them: 386; ASP; BAT; BIN; BMP; BOO; CHM; CLA; CLASS; CMD; CNM; COM; CPL; DEV; DLL; DO*; DRV; EML; EXE; GIF; HLP; HT*; INI; JPEG*; JPG; JS*; LNK; MD*; MSG; NWS; OCX; OV*; PCX; PGM; PHP*; PIF; PL*; PNG; POT; PP*; SCR; SHS; SMM; SYS; TIF; VBE; VBS; VBX; VXD; WMF; XL*; XML; ZL*;
- **Scan files without an extension** - If checked, the scan includes files without an extension.

Additional Options

Scan for Tracking Cookies - If checked, the scan includes internet browser tracking cookies. Found tracking cookies are deleted immediately and not moved to the virus vault.

Scan Potentially Unwanted Programs and Spyware threats - If checked, the scan detects executable applications or DLL libraries that could be potentially unwanted programs. Some programs, especially free ones, include adware and may be detected and reported by **Endpoint Security** as a **Potentially Unwanted Program**.

Scan files on close - If checked, files are scanned as they are closed.

Scan boot sector of removable media - If checked, the scan includes the boot sector of removable media.

Use Heuristics - If checked, scanning includes heuristic analysis. Heuristic analysis performs a dynamic emulation of a scanned object's instructions within a virtual computing environment.

Email Scanner

Enable Email Scanner - If checked, inbound and outbound email and attachments are scanned for viruses. If blank, no other **Email Protection** options are evaluated.

Note: Email Scanner is not recommended for *servers*. See the Exchange tab below.

Email Scanning

Check Incoming Email - If checked, incoming email is scanned.

Certification: Some email clients support appending text to email messages certifying that the email has been scanned for viruses.

- **Do Not Certify Email** - If selected, incoming email is not certified.
- **Certify all Email** - If selected, all incoming email is certified.
- **Only Certify Email with Attachments** - If selected, only incoming email with attachments are certified.
- **Incoming Email Certification** - Certification text appended to incoming email.

Check Outgoing Email - If checked, outgoing email is scanned.

- **Do Not Certify Email** - If selected, outgoing email is not certified.
- **Certify all Email** - If selected, all outgoing email is certified.
- **Only Certify Email with Attachments** - If selected, only outgoing email with attachments are certified.
- **Outgoing Email Certification** - Certification text appended to outgoing email.

Modify Subject for Messages Marked as Virus - Adds prefix text to the subject of a message that contains a virus.

Scanning Properties

Use Heuristics - Applies to an email message. If checked, scanning includes heuristic analysis. Heuristic analysis performs a dynamic emulation of a scanned object's instructions within a virtual computing environment.

Scan Potentially Unwanted Programs and Spyware threats - If checked, email scanning includes scanning for spyware, adware, and potentially unwanted programs.

Scan inside archives (RAR, RAR 3.0, ZIP, ARJ, CAB) - If checked, email archives are scanned.

Email Attachments Reporting (as a threat)

Report Password Protected Archives - If checked, reports password-protected archive attachments (zip, rar, etc) in email as threats.

Report Password Protected Documents - If checked, reports password-protected document attachments in email as threats.

Report Files containing macro - If checked, reports files containing macros attached to email as threats.

Report hidden extensions - If checked, reports files that use a hidden extension. Some viruses hide themselves by doubling their file extension. For example, the `VBS/Iloveyou` virus attaches a file, `ILOVEYOU.TXT.VBS`, to emails. The default Windows setting is to hide known extensions, so the file looks like `ILOVEYOU.TXT`. When you open it you do not open a `.TXT` text file but instead execute a `.VBS` procedure file.

Move reported attachments to Virus Vault (incoming email only) - If checked, reported email attachments are moved to the virus vault. They display in the **Virus Vault** tab of the **View Threats** (page 4) page instead of in the **Current Threats** tab.

Full Scan

Scan Settings

Scan Potentially Unwanted Programs and Spyware threats - If checked, the scan detects executable applications or DLL libraries that could be potentially unwanted programs. Some programs, especially free ones, include adware and may be detected and reported by **Endpoint Security** as a **Potentially Unwanted Program**.

Scan for Tracking Cookies - If checked, the scan includes internet browser tracking cookies. Found tracking cookies are deleted immediately and not moved to the virus vault.

Scan Inside Archives - If checked, scanning includes archive files—such as ZIP and RAR files.

Use Heuristics - If checked, scanning includes heuristic analysis. Heuristic analysis performs a dynamic emulation of a scanned object's instructions within a virtual computing environment.

Scan system environment - If checked, system areas are scanned before the full scan is started.

Scan infectible files only - If checked, "infectible" files are scanned based on their contents regardless of their file extensions. For example, an EXE file could be renamed but still be infected. The following types of files are considered 'infectible' files:

- **EXE type** - COM; DRV; EXE; OV?; PGM; SYS; BIN; CMD; DEV; 386; SMM; VXD; DLL; OCX; BOO; SCR; ESL; CLA; CLASS; BAT; VBS; VBE; WSH; HTA; HTM; HTML; ?HTML; CHM; INI; HTT; INF; JS; JSE; HLP; SHS; PRC; PDB; PIF; PHP; ZL?; ASP; LNK; EML; NWS; CPL; WMF
- **DOC type** - DO?; XL?; VBX; RTF; PP?; POT; MDA; MDB; XML; DOC?; DOT?; XLS?; XLT?; XLAM; PPT?; POT?; PPS?; SLD?; PPAM; THMX

Performance

Select System Priority for Scan - Defines how fast the scan runs and how much system resources the scan uses. You can set the scan to run as fast as possible while slowing down a computer noticeably, or you can choose that you wish the scan to run using as little system resources as possible, while prolonging the scan's run time.

Exchange

Enable AVG for Exchange Server - Enable or disable email scanning for assigned MS Exchange Servers.

Note: If you install email protection on one or more MS Exchange Servers, create a unique profile for MS Exchange Servers and only apply this profile to these MS Exchange Servers. The **Define Profile > Exchange** tab settings should only be enabled and applied to MS Exchange Servers.

Mail Certification - Enable or disable adding a certification note to scanned email on MS Exchange Servers. Customize the certification note in the text field.

Performance

Run scans in background - Enable or disable background scanning. Background scanning is one of the features of the VSAPI 2.0/2.5 application interface. It provides threaded scanning of the Exchange Messaging Databases. Whenever an item that has not been scanned before is encountered in users' mailbox folders, it is submitted to AVG for Exchange 2000/2003 Server to be scanned. Scanning and searching for unexamined objects runs in parallel. A specific low priority thread is used for each database, which guarantees other tasks, for example email messages storage in the Microsoft Exchange database, are always carried out preferentially.

Scan Proactively - Enable or disable VSAPI 2.0/2.5 proactive scanning. Proactive scanning involves dynamical priority management of items in the scanning queue. Lower priority items are not scanned unless all higher priority ones have been scanned. An item's priority rises if a client tries to use it, so an items' precedence changes dynamically according to user activity.

Scan RTF Files - Specify whether RTF files should be scanned or not.

Scanning Threads - The scanning process is threaded by default to increase the overall scanning performance by a certain level of parallelism. The default number of threads is computed as 2 times the 'number_of_processors' + 1.

Scan Timeout - The maximum continuous interval, in seconds, for one thread to access the message that is being scanned.

Exclude Dirs

Exclude Directories

Add new record - Adds directories excluded from a scan. Some directories may be threat-free but contain files that are erroneously interpreted as malware.

Warning: Do not exclude directories unless the contents of the directories are known to be threat-free.

Exclude PUPs

Exclude Potentially Unwanted Programs

Use this tab to exclude potentially unwanted programs, or PUPs, *manually*. The **View Threats** (page 11) page provides a quicker method of identifying and excluding PUPs.

Note: Non-PUP threats cannot be added to the PUP Exclusion List.

Add new record - Adds PUP files to exclude from a scan. Some files may be threat-free but be erroneously interpreted as potentially unwanted programs (PUPs). You need to identify the filename, its checksum value and its file size in bytes.

Warning: Do not exclude files unless the contents of the files are known to be threat-free.

Click **Add New Record** then enter the following:

- **Filename** - Enter the name of the file.
- **Checksum** - Enter the checksum value of the file. To determine the checksum value, open the **AVG UI** on a machine that contains the file. Select **Tools > Advanced Settings**. Select the **PUP Exceptions** property sheet. Click the **Add exception** button. Select the file by browsing the machine's local directory. The corresponding checksum value is displayed. Copy and paste the checksum value from the **AVG UI** into the **Add new record** dialog box of the **Exclude Pups** tab of Security > **Define Profile**.
- **File Size** - Enter the file size in bytes. To determine the file size, right-click the file in Windows Explorer and check the **Size** value in bytes.

Updates

Use this tab to configure how AVG updates are downloaded.

Proxy Settings

Enables/disables using a proxy server to download AVG updates.

- **Don't use proxy** - Disables proxy settings.
- **Use proxy** - Enables proxy settings.
- **Try connection using proxy, and if it fails, connect directly** - Enables proxy settings. If proxy fails, connects directly.

Manual - Sets proxy settings manually.

- **Server** - Enter a valid proxy server name or IP address.

- **Port** - Enter a port number.
- **Use PROXY authentication** - If checked, proxy authentication is required.
- **Username** - If **Use PROXY authentication** is checked, enter a valid username.
- **Password** - If **Use PROXY authentication** is checked, enter a valid password.

Auto - Sets proxy settings automatically.

- **From browser** - Select a default browser from the drop-down menu to set proxy settings.
- **From script** - Enter the full path of a script that specifies the proxy server address.
- **Auto detect** - Attempts to get the settings from the proxy server directly.

Update URL

AVG provides a default URL to download updates. You can preferentially download updates from a custom URL.

Use Custom Update URL - Select this option to preferentially download updates from a custom URL.

Name - Enter the name of the custom update URL.

URL - Enter the URL.

Assign Profile

Security > Assign Profile

The **Assign Profile** page assigns security profiles to machine IDs licensed to use **Endpoint Security**. Security profiles are defined using Security > **Define Profile** (page 20).

The list of machine IDs you can select depends on the machine ID / group ID filter. To display on this page, machine IDs must have the **Endpoint Security** client software installed on the managed machine using the Security > **Install/Remove** (page 16) page.

Apply Configuration

Click **Apply Configuration** to apply the security profile displayed in the **Select Profile** drop-down box to selected machine IDs.

Select Profile








Select a security profile to apply to selected machine IDs.


Only display machines with the selected profile

If checked, filters the paging area by the selected security profile.

Check-in 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

Note: Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

(Select All Checkbox)

Click this checkbox to select all rows in the paging area. If checked, click this checkbox to unselect all rows in the paging area.

Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Profile Name

Displays the security profile assigned to a machine ID. Displays the status of the machine ID if there is a problem.

Log Settings: Security

Security > Log Settings

The [Log Settings](#) page specifies the number of days to keep security protection log data for machine IDs licensed to use [Endpoint Security](#). Certain machines, such as web servers, may warrant maintaining a longer history of virus attacks than other types of machines.

The list of machine IDs you can select depends on the machine ID / group ID filter. To display on this page, machine IDs must have the [Endpoint Security](#) client software installed on the managed machine using the Security > [Install/Remove](#) (page 16) page.

Apply Configuration









Click [Apply Configuration](#) to apply the number of days specified in the [<N> days to keep log entries](#) field to selected machine IDs.

<N> days to keep log entries

Enter the number of days to maintain security protection log data.

Check-in 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

Note: Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

(Select All Checkbox)

Click this checkbox to select all rows in the paging area. If checked, click this checkbox to unselect all rows in the paging area.

Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Log Days Before Expiration

Shows the number of days security protection log data is maintained for a machine ID.

Exchange Status

Security > Exchange Status

The **Exchange Status** page displays the status of email protection on MS Exchange servers that have **Endpoint Security** installed on them. During the install of **Endpoint Security** on a machine, if MS Exchange is detected, the plugin for MS Exchange email protection is automatically installed.

Note: Any malware detected by MS Exchange Server email protection is immediately deleted from the MS Exchange Server and displays *only* on the Virus Vault tab of the **View Threats** (page 11) page.

The list of machine IDs you can select depends on the machine ID / group ID filter. Also, the machine ID must have MS Exchange Server installed on the machine.









Mailboxes Protected / Mailbox Licenses

Displays both the number of Exchange Server mailboxes protected and the number of mailbox licenses used and available.

Note: See **Endpoint Security Licensing in the Security Overview** (page ii) topic.

Check-in 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

Note: Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

(Select All Checkbox)

Click this checkbox to select all rows in the paging area. If checked, click this checkbox to unselect all rows in the paging area.

Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Install Status

If checked, [Endpoint Security](#) client software is installed on the machine ID. If the agent software is earlier than 4.7.1, the message `Requires Agent Update` displays. If blank, [Endpoint Security](#) client software is *not* installed on the machine ID.

Install Source

If a file source is defined using Patch Management > File Source, then installs are sourced from this location. Otherwise, installs are sourced from the internet.

If the option [Download from Internet if machine is unable to connect to the file server](#) is selected in Patch Management>File Source:

- During a [Endpoint Security](#) v2.x endpoint install, if the files source is down or credentials invalid, the installer is downloaded from the Kserver and completes the endpoint install.
- During a [Endpoint Security](#) v2.x manual update, if the files source is down or credentials invalid, the update is downloaded from the internet.

In both cases above, the [View Logs](#) (*page 13*) page displays an error message stating why the file source failed and that it is trying to download from the internet.

Mailboxes

The number of email accounts on the MS Exchange Server.

Installed On

The date MS Exchange Server email protection was installed on the machine ID.

Define Alarm Sets

Security > Define Alarm Sets

The [Define Alarm Sets](#) page defines sets of alarm conditions used to trigger alerts using the [Apply Alarm Sets](#) (*page 30*) page.

This page provides the following actions:

- [Save](#) - Save the alarm set.
- [Save As](#) - Save an alarm set to a new name.
- [Delete](#) - Delete an alarm set.
- [Share](#) - Displays if you own a selected alarm set. Share this alarm set with users, user roles or to make public for all users. Share rights are assigned *by object*. There are three sharing checkbox options. The first two checkboxes are *mutually exclusive* and determine what share rights are assigned. If neither of the first two checkboxes are checked, the shared object can only be seen by the users given share access, but the object cannot be used nor edited. The [Shared](#) and [Not Shared](#) list boxes and the third checkbox determine who can see the object.

- **Allow other administrators to modify** - If checked, share rights to the object includes being able to use it, view its details and edit it.
- **Other administrators may use but may not view or edit** - If checked, share rights to the object only allows using it.
- **Make public (seen by all administrators)** - If checked, ensures that *all* current and future VSA users can see the object. If blank, only selected user roles and users can see the shared object. If blank, and new users or user roles are added later, you have to return to this dialog to enable them to see the specific object.
- **Take Ownership** - Displays if you do not *own* a selected public alarm set. Click to take ownership and make changes to the alarm set. This option only displays for master role users.

To Create a New Alarm Set

1. Select <No Alarm Sets Saved> in the **Select Profile** drop-down list. Alternatively you can select an existing alarm set and click **Save As**.
2. Check one or more alarm condition checkboxes.
3. Use the **Ignore additional alarms for <N> <periods>** to specify the number of minutes to ignore the same set of alarm conditions. Set to 0 to trigger an alarm each time an alarm condition occurs.
4. Click **Save** to save the alarm set.

To Delete an Alarm Set

1. Select an alarm set from the **Select Profile** drop-down list.
2. Click **Delete** to delete the alarm set.

Ignore additional alarms <N> <periods>

Specify the number of periods you want the same type of alarm to be ignored after the first alarm is triggered.

Alarm Conditions

Check any of the following types of alarm conditions to include it in a **Endpoint Security** alarm set.

- **Threat Detected and Not Healed** - A threat has been added to the **Current Threats** tab of the **View Threats** (*page 11*) page that could not be automatically healed
- **Protection Disabled** - Security protection has been disabled.
- **Definition Updated** - Security protection has been updated with the latest version of **Endpoint Security**.
- **Scheduled Scan Completed** - A security protection scan has been completed.
- **Reboot Required** - A reboot is required.
- **Protection Enabled** - Security protection has been enabled.
- **Service Error** - The **Endpoint Security** service has stopped.
- **Definition Not Updated in <N> Days** - Security protection has not been updated for the specified number of days.
- **Scheduled Scan Did Not Complete** - A scheduled security protection scan did not complete.
- **AVG Removed by User** - A machine user has uninstalled the AVG client from the managed machine.

Apply Alarm Sets

Security > Apply Alarm Sets

The **Apply Alarm Sets** page creates alerts in response to security protection alarm conditions defined using **Define Alarm Sets** (*page 29*). The alarms sets are applied to selected machine IDs licensed to use **Endpoint Security**.

The list of machine IDs you can select depends on the machine ID / group ID filter. To display on this page, machine IDs must have the **Endpoint Security** client software installed on the managed machine using the Security > **Install/Remove** (page 16) page.

The page provides you with four actions:

- **Apply** - Apply a selected alarm set to selected machine IDs.
- **Remove** - Remove a selected alarm set from selected machine IDs.
- **Remove All** - Remove all alarm sets assigned to selected machine IDs.
- **Format Email** - Format the email sent to email recipients. This option only displays for master role users.

To Create an Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:
 - Create **Alarm**
 - Create **Ticket**
 - Run **Script**
 - **Email Recipients**
2. Set additional email parameters.
3. Select an alarm set.
4. Check the machine IDs to apply the alarm set to.
5. Click **Apply** to assign the alarm set to selected machine IDs.

To Cancel an Alert

1. Select machine ID checkboxes.
2. Click **Remove** to remove the assigned alarm set from selected machine IDs.

Passing Alert Information to Emails and Procedures

The following types of **Apply Alarm Sets** alert emails can be sent and formatted:

- Security Alarm

Note: Changing this email format changes the format for *all Apply Alarm Sets alert emails*. You may need to greatly restrict the size of an email alarm message if the destination email address is a pager or some hand-held device.

The following variables can be included in your formatted email alerts.

Within an Email	Within a Procedure	Description
<as>	#as#	KES alarm set
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<sm>	#sm#	security alarm
<st>	#st#	security alarm specific title

<tk>	#tk#	ticket ID
<ty>	#ty#	security alarm type
	#subject#	subject text of the email message, if an email was sent in response to an alarm
	#body#	body text of the email message, if an email was sent in response to an alarm

Create Alarm

If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Script

If checked and an alarm condition is encountered, an agent procedure is run. You must click the [select agent procedure](#) link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking [this machine ID](#) link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, emails are sent to the specified email addresses.









- Click [Format Email](#) to display the [Format Alert Email](#) popup window. This window enables you to format the display of emails generated by the system when an alarm is triggered. See [Passing Alert Information to Emails and Procedures](#) above. This option only displays for master role users.
- Email is sent directly from the VSA to the email address specified in the alert. Set the [From Address](#) using System > Outbound Email.

Select an Alarm Set

Select an alarm set to apply to selected machine IDs.

Check-in 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

Note: Different icon images display when this add-on module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

(Select All Checkbox)

Click this checkbox to select all rows in the paging area. If checked, click this checkbox to unselect all rows in the paging area.

Machine.Group ID

The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Alarm Set

Lists the alarm sets assigned to each machine ID.

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

- A = Create **A**larm
- T = Create **T**icket
- S = Run Agent Procedure
- E = **E**mail Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

Security Reporting in VSA 5.x

All security protection events are logged within the system and available for executive summary and detailed management reporting.

Executive Summary

The Reports > Executive Summary report includes a section called **Endpoint Security Last N Days**. It includes the following statistics.

- Total threats detected
- Current Active Threats
- Current Threats in Vaults
- Threats Resolved
- Scans Completed
- Updates Performed
- Machines with KES installed

The **Network Health Score** of the **Executive Summary** includes an **Endpoint Score** category. Untreated threats are the threats that are listed on the **Current Threats** tab of the Security > **View Threats** (page 11) page. Untreated threats represent potential system problems. The number of untreated threats generated by each machine over the specified period of time is scored as follows:

0 untreated threats	100%
1 to 4 untreated threats	75%
5 to 10 untreated threats	50%
more than 10 untreated threats	25%

You can adjust how heavily each category effects the total **Network Health Score** by adjusting the **weight** value for each category. Weights range from 0 to 100. Set the weight to zero to turn off that category.

Security Log

The Reports > [Logs](#) page generates reports for log data maintained by the VSA, including the `EPS log`.

Security Report

The Reports > Security page generates reports for [Endpoint Security](#) protected machines, including [Configuration Report](#), [Current Threats](#) and [Historical Threats](#).

Security Reporting in VSA 6.x

All security protection events are logged within the system and available for executive summary and detailed management reporting.

Executive Summary

The Info Center > Reports > Executive Summary report includes a section called [Endpoint Security Last N Days](#). It includes the following statistics.

- Total threats detected
- Current Active Threats
- Current Threats in Vaults
- Threats Resolved
- Scans Completed
- Updates Performed
- Machines with KES installed

The [Network Health Score](#) of the [Executive Summary](#) includes an [Endpoint Score](#) category. Untreated threats are the threats that are listed on the [Current Threats](#) tab of the Security > [View Threats](#) (*page 11*) page. Untreated threats represent potential system problems. The number of untreated threats generated by each machine over the specified period of time is scored as follows:

0 untreated threats	100%
1 to 4 untreated threats	75%
5 to 10 untreated threats	50%
more than 10 untreated threats	25%

You can adjust how heavily each category effects the total [Network Health Score](#) by adjusting the [weight](#) value for each category. Weights range from 0 to 100. Set the weight to zero to turn off that category.

Security Log

The Info Center > Reports > Logs - [KES Log](#) report definition generates a report of [Endpoint Security](#) log entries by machine ID.

Security Report

The Info Center > Reports > [Security](#) report definition generates reports of [Endpoint Security](#) protected machines, including [Configuration](#), [Current Threats](#) and [Historical Threats](#).

Index

A

Apply Alarm Sets • 30
Assign Profile • 26

D

Dashboard • 3
Define Alarm Sets • 29
Define Profile • 20

E

Enable/Disable Resident Shield by Agent Procedure •
6
Exchange Status • 28
Extend/Return • 13

I

Install/Remove
Security • 16

L

Log Settings
Security • 27

M

Manual Update • 7

N

Notify • 15

S

Schedule Scan • 10
Security Overview • 1
Security Reporting in VSA 5.x • 33
Security Reporting in VSA 6.x • 34
Security Status • 4

V

View Logs • 13
View Threats • 11