Kaseya Endpoint Security

User Guide

Version 2.0

January 28, 2009

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

Chapter 1

Security

In This Chapter

Security Tab

Kaseya 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. Kaseya Endpoint Security automatically cleans or removes infected files and other threats such as trojans, worms and spyware. Kaseya 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 scripts, 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. 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.

> Note: You can view Kaseya Endpoint Security demos at http://www.kaseya.com/Demo.aspx
>
> Note: You can view a Kaseya Endpoint Security training video at https://training.kaseya.com
> https://training.kaseya.com

Anti-Virus Protection

Based on the security profile, Kaseya 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 mail 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 electronic mail, 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. Kaseya Endpoint Security comes with a pre-defined standard security profile and enables you to create customized security profiles.
- Scans MS Exchange Servers - Scans inbound and outbound e-mail 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.

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 Kaseya Endpoint Security spyware component. A memory resident shield scans applications in the background as they run. Kaseya 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.

Functions	Description
Security Status *(page 8)*	Displays the current security status of machine IDs.
Manual Updates *(page 7)*	Schedules updates of latest version of security protection definition files.
Schedule Scan *(page 8)*	Schedules security protection scans of machine IDs.
View Threats *(page 10)*	Lists files that have been placed in quarantine due to a suspicious or confirmed threat.
View Logs *(page 11)*	Displays the security protection event log of machine IDs.
Extend/Return *(page 12)*	Extends the annual license count for selected machines IDs or returns annual licenses from selected machine IDs.
Notify *(page 13)*	Provides automatic notification of the expiration of Endpoint Security licenses.
Install/Remove *(page 14)*	Installs or removes security protection for machine IDs.
Define Profile *(page 17)*	Manages security profiles. Each security profile represents a different set of of enabled or disabled security options.
Assign Profile *(page 21)*	Assigns security profiles to machine IDs.
Log Settings *(page 22)*	Specifies the number of days to keep security protection log data.
Install/Remove *(page 23)*	Installs or removes email protection for MS Exchange Server machines.
Define Alarm Sets *(page 25)*	Defines sets of alarm conditions used to trigger alerts using the Apply Alarm Sets page.
Apply Alarm Sets *(page 26)*	Creates alarms in response to security protections events.

Security Status

Security > Security Status

- Similar information is provided by Reports > Security.

The Security Status page displays the current security status of each machine ID licensed to use Kaseya Endpoint Security. The list of machine IDs displayed depends on the Machine ID / Group ID filter and machine groups the administrator is authorized to see using System > Group Access. To display on this page, machine IDs must have the Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 14)* 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.

The page provides you with the following actions:

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

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

- Enable Email - Click to enable email protection on selected machines.
- Disable Email - Click to disable email protection on selected machines.
- Empty Vault - Click to empty the virus vault of all quarantined malware.

Current Available 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 26)*.

Check-in status

These icons indicate the agent check-in status of each managed machine:

 Agent has checked in

 Agent has checked in and user is logged on. Tool tip lists the logon name.

 Agent has not recently checked in

 Agent has never checked in

 Online but waiting for first audit to complete

 The agent is online but remote control is disabled

 The agent has been suspended

(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 ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Profile Name

The security profile assigned to the machine ID.

Resident Shield

If the resident-memory, green-check icon  displays, resident-memory protection is enabled on the machine ID. If a resident memory red-X icon  displays, resident-memory protection is not enabled on the machine ID.

Email Scanner

If the email green-check icon  displays, email protection is enabled on the machine ID. If an email red-X icon  displays, email protection is not enabled on the machine ID.

Threats

The number of unhealed threats detected on the machine ID. These are current threats that need administrator attention. You can click the hyperlinked number in any row to display these threats in the Current Threats tab of the View Threats *(page 10)* 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 10)* > page.

Version

The version of security protection currently used by the machine ID. If the version number is less than the Current Available Version, the machine ID's security protection needs to be updated using Security > Manual Updates *(page 7)*. Typically security protection is updated automatically.

Manual Update

Security > Manual Update

The Manual Updates page updates machine IDs licensed to use Kaseya Endpoint Security with the latest version of security protection available. Updates are scheduled automatically. 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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 14)* page.

The page provides you with the following actions:

- Update - Click to schedule an update of selected machine IDs using the update options previously selected.
- Cancel Update - Click to clear a scheduled update.

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:

 Agent has checked in

 Agent has checked in and user is logged on. Tool tip lists the logon name.

 Agent has not recently checked in

 Agent has never checked in

 Online but waiting for first audit to complete

 The agent is online but remote control is disabled

 The agent has been suspended

(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 ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Source

If a file source is defined using Patch Mgmt > 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 an KES v2.0 endpoint install, if the files source is down or credentials invalid, the installer is pulled down from the Kserver and completes the endpoint install.
- During an KES v2.0 manual update, if the files source is down or credentials invalid, the update is pulled from the internet.

In both cases above, the View Logs *(page 11)* page displays an error message stating why the file source failed and that it is trying to download through 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.

Scheduled Time

Timestamp showing the next scheduled update.

Schedule Scan

Security > Schedule Scan

The Schedule Scan page schedules security protection scans of selected machine IDs licensed to use Kaseya 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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 14)* page.

The page provides you with 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 times to run this task each time period.

Check-in status

These icons indicate the agent check-in status of each managed machine:

 Agent has checked in

 Agent has checked in and user is logged on. Tool tip lists the logon name.

 Agent has not recently checked in

 Agent has never checked in

 Online but waiting for first audit to complete

 The agent is online but remote control is disabled

 The agent has been suspended

(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 ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Last Scan

This timestamp shows when a machine ID was last scanned. When this date changes, new scan data is available to view.

Next Scan / Schedule

This timestamp shows the next scheduled scan. It also indicates if the schedule is recurring.

View Threats

Security > View Threats

- Similar information is provided by 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 administrator action. Deleting a threat on the Current Threats tab deletes the file immediately, without moving the file to the Virus Vault.
- 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 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.
- Cancel Pending Operation - Cancels any of the other actions, if they have not yet been completed.
- Add to PUP Exclusion List - Selected threats are 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 17)* > PUP Exclusions tab.

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.
- Cancel Pending Operation - Cancels any of the other actions, if they have not yet been completed.

- Add to PUP Exclusion List - Selected threats are 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 PUP Exclusion List is maintained using the Define Profile *(page 17)* > PUP Exclusions tab.

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.
- Actions - 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 Reports > Security.

The View Logs page displays the security protection event log of each machine ID licensed to use Kaseya Endpoint Security. The list of machine IDs displayed depends on the Machine ID / Group ID filter and machine groups the administrator is authorized to see using System > Group Access. To display on this page, machine IDs must have the Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 14)* 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.

- Time, Min, Max - Filter by a range of dates and times.

- Category - Filter by the type 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.

Each installation of security protection on a managed machine uses up one annual Kaseya Endpoint Security license. The number of annual licenses available depends on the total number of annual licenses purchased and allocated to each group ID. Licenses are allocated to group IDs using System > License Manager.

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 14)* 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.

Licenses Used

Displays the number of annual Kaseya 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 KES 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 KES license.

(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 ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

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.

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 administrator that more annual licenses may be required for that group ID. Kaseya 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, users and administrators can be notified a specified number of days before security protection licenses expire.

Each installation of security protection on a managed machine uses up one annual Kaseya Endpoint Security license. The number of annual licenses available depends on the total number of annual licenses purchased and allocated to each group ID. Licenses are allocated to group IDs using System > License Manager.

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 14)* 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 administrators.

Email Recipients (Comma separate multiple addresses)

Specify email addresses to send notification messages. Multiple email addresses must be separated by commas. You can set the From Address for all emails created by the VSA using the System > Configure page.

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:

- Agent has checked in
- Agent has checked in and user is logged on. Tool tip lists the logon name.
- Agent has not recently checked in
- Agent has never checked in
- Online but waiting for first audit to complete

 The agent is online but remote control is disabled

 The agent has been suspended

Machine.Group ID

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

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 forwarned 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 administrator is authorized to see using System > Group Access. Installation requires a reboot of the managed machine.

Each installation of security protection on a managed machine uses up one annual Kaseya Endpoint Security license. The number of annual licenses available depends on the total number of annual licenses purchased and allocated to each group ID. Licenses are allocated to group IDs using System > License Manager.

The page provides you with four actions:

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

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

- Remove - Remove Kaseya 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.

Options

Click Options to configure the following installation options.

Install Options

- User Name - If checked, enter a name associated with this install of Kaseya Endpoint Security.
- Company Name - If checked, enter the name of the company associated with this install of Kaseya 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.
- 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 administrator 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.
- Install AVG Toolbar - If checked, installs the AVG Toolbar to the following:
  - Microsoft Windows 2000
  - Microsoft Windows XP
  - Microsoft Windows Vista (32-bit)
  - Microsoft Internet Explorer (version 6.0 or greater)
  - Mozilla FireFox (version 1.5 or greater)
- Does not install to browsers running on Windows Server O/S.
- MS Office 2000 - 2007 Add-in - Installs the AVG scanning plugin for Microsoft Office, versions 2000 though 2007.
- Email Scanner - If checked, installation detects the default email client on a machine and automatically installs the respective email scanning plug-in.
- 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.

> 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.*

- 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.
  - Surf-Shield - Scans a link displayed in a web page, before you click it.
  - Active 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.

Script Options

- Script to run before install. Select a script.
- Script to run after install. Select a script.

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 Kaseya Endpoint Security licenses applied to machines.

License Pool

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

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:

- Agent has checked in
- Agent has checked in and user is logged on. Tool tip lists the logon name.
- Agent has not recently checked in
- Agent has never checked in
- Online but waiting for first audit to complete
- The agent is online but remote control is disabled
- The agent has been suspended

(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 ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Install Status

If checked, Kaseya 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, Kaseya Endpoint Security client sofware is *not* installed on the machine ID.

Install Source

If a file source is defined using Patch Mgmt > 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 an KES v2.0 endpoint install, if the files source is down or credentials invalid, the installer is pulled down from the Kserver and completes the endpoint install.
- During an KES v2.0 manual update, if the files source is down or credentials invalid, the update is pulled from the internet.

In both cases above, the View Logs *(page 11)* page displays an error message stating why the file source failed and that it is trying to download through the internet.

Installed On

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

Expires On

The date Kaseya Endpoint Security licensing is scheduled to expire on the machine ID.

Define Profile

Security > Define Profile

The Define Profile page manages security profiles. Each security profile represents a different set of 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 21)*. Typically different types of machines or networks require different security profiles.

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 administrators, except for master administrators, cannot see private security profiles. Sharing a private security profile makes it a public security profile.
- Take Ownership - Takes ownership of any public security profile.

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

3. Click the Save or Save As button to save the security profile.

General

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.

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 administrator can also enable/disable security protection remotely using Security > Security Status *(page 5)*.

Run System Scan upon KES Start Up - If checked, security protection scans the following system areas on startup:

- Boot sector of disk
- Master boot record in the partition table
- System registry
- System32 files: kernel32.dll, wsock32.dll, user32.dll, shell32.dll, ntoskrnl.exe
- System32\Drivers

Resident Shield

Resident shield is a memory-resident feature.

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

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.

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 Kaseya 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 Protection

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 scanning applies to local email clients, such as Outlook, installed on the managed machine. It does not apply to email scanning for MS Exchange Servers. See the Exchange section below.

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.

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.

Report Password Protected Attachments - If checked, reports password-protected attachments to emails as threats.

Report Password Protected Documents - If checked, reports password-protected documents as emails as threats.

Report Files containing macro - If checked, reports files containing macros attached to emails 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 e-mails. 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 script 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 5)* page instead of in the Current Threats tab.

Full Scan

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 Kaseya 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

Scan for rootkits - If checked, scans for rootkit viruses. A rootkit virus attempts to take control of a machine using "Administrator" or "System" level access without authorization by the system's owners and legitimate managers.

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 noticably, 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.

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 the 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

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

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

Assign Profile

Security > Assign Profile

The Assign Profile page assigns security profiles to machine IDs licensed to use Kaseya Endpoint Security. Security profiles are defined using Security > Define Profile *(page 17)*.

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 14)* 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:

- Agent has checked in
- Agent has checked in and user is logged on. Tool tip lists the logon name.
- Agent has not recently checked in
- Agent has never checked in
- Online but waiting for first audit to complete
- The agent is online but remote control is disabled
- The agent has been suspended

(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 ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Profile Name

Displays the security profile assigned to a machine ID.

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 Kaseya Endpoint Security. Certain machines, such as web servers, may warrant maintaining a longer history of virus attacks then 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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 14)* 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 in the N days to keep log entries field.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Agent has checked in
- Agent has checked in and user is logged on. Tool tip lists the logon name.

- Agent has not recently checked in
- Agent has never checked in
- Online but waiting for first audit to complete
- The agent is online but remote control is disabled
- The agent has been suspended

(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 ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Log Days Before Expiration

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

Install/Remove: MS Exchange

Security > Install/Remove: MS Exchange

The MS Exchange Install/Remove page installs, removes, or re-installs email protection on selected MS Exchange Server machine IDs.

> Note: Any malware detected by MS Exchange Server email protection is immediately deleted from the MS Exchange Server and displays *only* on the Historical Threats tab of the View Threats *(page 10)* page.

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 14)* page. Also, the machine ID must have MS Exchange Server installed on the machine.

The page provides you with four actions:

- Install - Install MS Exchange Server email protection on selected machine IDs.
- Remove - Remove MS Exchange Server email protection on selected machine IDs.
- Cancel Pending Operation - Cancel either of the first two actions, if they have not yet been completed.

Mailbox Licensing

Each KES license you purchase gives you one endpoint license for a year, and one "mailbox-seat" worth 365 days of protection on a single Exchange mailbox. Protected mailboxes are counted on a daily basis. The total number of protected mailboxes, both public and normal, are counted via the Active Directory environment. A protected mailbox is counted whether it is used or not. The system keeps a count of the number of "mailbox-days" of usage across all protected mailboxes.

Example

Mailbox-Seats Used: 63.25 out of 4500 on 1797 mailboxes

- 63.25 is the number of mailbox-seats used so far, calculated as mailbox-days / 365.
- 1797 is the number of Exchange mailboxes currently under protection, calculated by counting mailboxes on Exchange servers where the MS Exchange component is installed.

- 4500 is the number of mailbox-seats purchased, equal to the number of KES licenses purchased.
- (4500 mailbox-seats - 63.25 mailbox-seats used so far) / 1797 mailboxes = 2.47 years, the estimated time mailbox protection will expire based on the current number of mailboxes deployed and rate of usage.

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.

Mailbox-Seats Used

Displays both the number of Exchange Server mailbox-seats available and the number of mailbox-seats currently protected.

Check-in status

These icons indicate the agent check-in status of each managed machine:

 Agent has checked in

 Agent has checked in and user is logged on. Tool tip lists the logon name.

 Agent has not recently checked in

 Agent has never checked in

 Online but waiting for first audit to complete

 The agent is online but remote control is disabled

 The agent has been suspended

(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 ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Install Status

If checked, Kaseya 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, Kaseya Endpoint Security client sofware is *not* installed on the machine ID.

Install Source

If a file source is defined using Patch Mgmt > 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 an KES v2.0 endpoint install, if the files source is down or credentials invalid, the installer is pulled down from the Kserver and completes the endpoint install.
- During an KES v2.0 manual update, if the files source is down or credentials invalid, the update is pulled from the internet.

In both cases above, the View Logs *(page 11)* page displays an error message stating why the file source failed and that it is trying to download through 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 26)* page.

The page provides you with 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 administrators, administrator roles or to make public for all administrators.
- Take Ownership - Displays if you do *not* own a selected public alarm set. Click to take ownership and make changes to the alarm set.

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 an alarm set for machines that have Kaseya Endpoint Security installed on it.

- Threat Detected and Not Healed - A threat has been added to the Current Threats tab of the View Threats *(page 10)* 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 Kaseya 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 Kaseya Endpoint Security service has stopped.
- Definition Not Updated in <N> Days - Security protection scan not been updated in the specified number of days.
- Scheduled Scan Did Not Complete - A scheduled security protection scan did not complete.

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 25)*. The alarms sets are applied to selected machine IDs licensed to use Kaseya 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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 14)* page.

The page provides you with four actions:

- Apply - Apply parameters to selected machine IDs.
- Remove - Remove a select 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.

To Create an Alert

1. Check any of these checkboxes to perform their corresponding actions when a 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 Scripts

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 and in scripts.

Within an Email	Within a Script	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 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, a script is run. You must click the select script link to choose a script to run. You can optionally direct the script to run on a specified range of machine IDs by clicking the this machine ID link. These specified machine IDs do not have to match the machine ID that triggered the alarm.

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 Scripts above.
- Email is sent directly from the VSA to the email address specified in the alert. The SMTP service in IIS 4 or 5 sends the email directly to the address specified. Set the From Address using the System > Configure page.

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:

 Agent has checked in

 Agent has checked in and user is logged on. Tool tip lists the logon name.

 Agent has not recently checked in

 Agent has never checked in

 Online but waiting for first audit to complete

 The agent is online but remote control is disabled

 The agent has been suspended

(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 ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

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 Alarm
- T = Create Ticket
- S = Run Script
- E = Email Recipients

Email Address

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

Security Reporting

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.

- Threats Detected
- Threats Cleaned
- Threats Restored
- Threats Deleted
- Threats Quarantined
- Threats Failed to Clean
- Threats Failed to Restore
- Threats Failed to Delete
- Threats Failed to Quarantine
- Threats With No Action
- Threats Action Pending
- 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 10)* 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 KES protected machines, including Security Profile Configuration, Current Threats and Historical Threats.

Index