Kaseya Endpoint Security

User Guide

September 6, 2007

© Copyright 2000-2007 Kaseya, All rights reserved.
Names and products mentioned may be trademarks or registered trademarks of their respective owners.

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 Grisoft AVG. 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.

Anti-Virus Protection

Based upon 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.
- On Access 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. On Access Protection, loaded in the memory of the computer during system startup, also 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 pre-defined security profiles and enables you to create customized security profiles.

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 5)*	Displays the current security status of machine IDs.
Schedule Scan *(page 5)*	Schedules security protection scans of machine IDs.
Enable/Disable *(page 6)*	Allows administrators to start or stop security protection of machine IDs.
View Threats *(page 7)*	Lists files that have been placed in quarantine due to a suspicious or confirmed threat.
View Logs *(page 8)*	Displays the security protection event log of machine IDs.
Install/Remove *(page 11)*	Installs or removes security protection for machine IDs.
Define Profile *(page 13)*	Manages security profiles. Each security profile represents a different set of of enabled or disabled security options.
Assign Profile *(page 19)*	Assigns security profiles to machine IDs.
Log Settings *(page 20)*	Specifies the number of days to keep security protection log data.
Updates *(page 21)*	Schedules updates of latest version of security protection definition files.
Security Alarms *(page 23)*	Creates alarms in response to security protections events.

Agent Menu Security Options

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

If Allow user to enable/disable Security Protection in agent task menu is checked in the General tab in Security > Define Profile *(page 13)*:

- 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.

The administrator can also enable/disable security protection from the VSA console using Security > Enable/Disable *(page 6)*.

Security Status

Security > Security Status

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. To display on this page, machine IDs must have Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 11)* page.

Indicators include general security protection, file protection, mail protection, the number of threats detected, and the version of security protection installed on each machine ID.

Current Signature Version

The latest version of security protection available. You can update one or more machine IDs with the Current Signature Version using Security > Updates *(page 23)*.

Check-in status

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

- Agent has checked in
- 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

Machine ID.Group ID

The list of Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

Profile Name

The security profile assigned to the machine ID.

Protection

If checked, security protection is enabled on the machine ID.

File

If checked, file protection is enabled on the machine ID.

Mail

If checked, email protection is enabled on the machine ID.

Threats

The number of threats detected on the machine ID.

Version

The version of security protection currently used by the machine ID. If the signature version is less than the Current Signature Version available, the machine ID's security protection needs to be updated using Security > Updates *(page 23)*.

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 11)* page.

Scan

Click Scan to schedule a scan of selected machine IDs using the scan options previously selected.

Cancel

Click Cancel 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 Stagger by for 5 minutes, then the scan 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. If the machine is offline, skip and reschedule for the next day at the same 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 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

Machine ID.Group ID

The list of Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

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.

Enable/Disable

Security > Enable/Disable

The Enable/Disable page allows administrators to start or stop security protection of selected machine IDs licensed to use Kaseya Endpoint Security. Disabling security protection may be required to install or configure certain software on the managed machine. If users on managed machines are not provided the option of manually turning the Kaseya Endpoint Security client software on or off themselves, an administrator can perform this task using this page.

Note: This user option is set using the Allow user to enable/disable Security Protection in agent task menu box in the General tab of Security > Define Profile *(page 13)*.

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 11)* page.

Enable

Click Enable to turn on security protection on selected machine IDs.

Disable

Click Disable to turn off security protection on selected machine IDs.

Check-in status

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

- Agent has checked in
- 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

Machine ID.Group ID

The list of Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

Protection

If checked, security protection is enabled on the machine ID.

View Threats

Security > View Threats

The View Threats page lists files that have been placed in quarantine due to a suspicious or confirmed threat. The page provides you with four actions:

- Restore As Is - Restore the file from quarantine and make no changes to it.
- Attempt to Clean & Restore - Attempt to remove the malware infecting the file, then restore the file.
- Delete - Delete the file.
- Cancel Pending Operation - Cancel any of the other actions, if they have not yet been completed.

Attempting to Clean & Restore and Delete may take some time. Restore As Is is relatively quick. All three actions, if successful, removes the threat from this list.

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

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.

Apply Filter / Reset Filter

Click Apply Filter to filter the rows displayed by the text entered in either the File Path or Threat Name fields. Click Reset Filter to display all rows of data.

File Path / Threat Name Filter Fields

Enter *starting* text to filter the rows of data displayed. You can also enter a wildcard asterisk (*) to the left of a string or insert a wildcard asterisk in the middle of a string to display all rows of data matching these expressions.

Machine.Group

Lists Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

File Path

The full pathnames of quarantined files.

Threat Name

The threat names used to classify quarantined files.

Action

The status of actions taken to dispose of quarantined files.

View Logs

Security > View Logs

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. To display on this page, machine IDs must have Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 11)* page.

Click a machine ID.group ID to display an event log. Each event displays the Time, an even Code, and in most cases a Message containing additional information. Types of security protection event codes include:

- CommandProcessed
- CommandReceived
- FullScanCancelled
- FullScanCompleted
- FullScanStarted
- ScanProgress
- ThreatCleanFailed
- ThreatDeleted
- ThreatDetected
- ThreatMissing
- ThreatQuarantined

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. Partial years cannot be returned.

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 11)* page.

The page provides you with two 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 and available.

Machine ID.Group ID

The list of Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 11)* 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 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

Machine ID.Group ID

The list of Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

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. 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 Prompt - 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 security protection installation.

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 Stagger by for 5 minutes, then the scan 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. If the machine is offline, skip and reschedule for the next day at the same time. Uncheck to perform this task as soon as the machine connects after the scheduled time.

Licenses Used

Displays the number of annual Kaseya Endpoint Security licenses used and available.

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 Prompt 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 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

Machine ID.Group ID

The list of Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

Install Source

Identifies the source location the Kaseya Endpoint Security client software is downloaded from.

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.

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 19)*. Typically different types of machines or networks require different security profiles.

The page provides you with four 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 - Take 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
   - File Protection
   - Mail Protection
   - Full Scan
   - Exclude Dirs
3. Click the Save or Save As button to save the security profile.

General

Keep files in quarantine for this many days before deleting - Enter the number of days to store quarantined threats before they are automatically deleted.

Minimum MB To preserve on disk - Enter the minimum number of megabytes to allocate on the disk to the storage of quarantined threats.

Maximum per

centage of disk used - Enter the maximum percentage of disk space to allocate for the storage of quarantined threats.

Allow user to enable/disable Security Protection in agent task 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 > Enable/Disable *(page 6)*.

Scan System Areas on Startup - 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

File Protection

File protection is a memory resident feature. Files are scanned for viruses as they are copied, opened or saved on the managed machine.

Enable File Protection - If check, the following types of files are scanned as they are copied, opened or saved.

386; ASP; BAT; BIN; BMP; BOO; CHM; CLA; CLAS*; 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 all files - If selected, all files on the managed machine are scanned.

Scan programs and documents (by extension) - If selected, specifies the file extensions of programs and documents to include or exclude.

Exclude files with these extensions - 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.

Also scan files without an extension - If checked, the scan includes files without an extension.

Scan floppy drives - If checked, the scan includes floppy drives.

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

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

Scan potentially unwanted programs - 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 cookies - If checked, the scan includes internet browser cookies.

Once detected an infected file can be moved or deleted, but it cannot be opened, saved or copied. Use the following list to determine how to set the Disinfect and Delete checkboxes:

- Disinfect Yes / Delete Yes - An attempt is made to clean the original file. If cleaning fails, the original file is deleted. The file is not quarantined.
- Disinfect Yes / Delete No - An attempt is made to clean the original file. If cleaning fails the original file is moved to quarantine and the original file displays in the Security > View Threats page. If the original file is deleted using the View Threats page, both the quarantined copy and the original file are deleted.
- Disinfect No / Delete Yes - No attempt is made to clean the original file. The original file is deleted without putting a copy of the original file in quarantine.
- Disinfect No / Delete No - No attempt is made to clean or delete the file. The original file displays in the Security > View Threats page as infected.

Mail Protection

Enable Mail Protection - If checked, inbound and outbound email and attachments are scanned for viruses.

Check Incoming Mail - 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 - If selected, incoming email is not certified.

Certify all mail - If selected, all incoming email is certified.

Certify mail with attachments only - If selected, only incoming email with attachments are certified.

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

Do Not Certify - If selected, outgoing email is not certified.

Certify all mail - If selected, all outgoing email is certified.

Certify mail with attachments only - If selected, only outgoing email with attachments are certified.

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

Enable Anti-Spyware engine - If checked, email scanning includes scanning for spyware, adware, and potentially unwanted programs.

Scan Inside Archives - If checked, email archives are scanned.

Automatically move password-protected archives to quarantine - Automatically quarantines password-protected archives. Password-protected archives may contain virus/spyware/malware threats. You can recover password-protected archives using the Security > View Threats *(page 7)* page.

Remove all attached executable files - If checked, executables files, whether infected or not, are removed from email.

Remove all attached documents - If checked, attachments, whether infected or not, are removed from email.

Remove files with these extensions - Enter the extensions of files that should be automatically removed from email. Enter each extension separated by a semi-colon (;) character.

> Note: The term file in the following discussion refers to an individual email message.

Once detected an infected file can be moved or deleted, but it cannot be opened, saved or copied. Use the following list to determine how to set the Disinfect and Delete checkboxes:

- Disinfect Yes / Delete Yes - An attempt is made to clean the original file. If cleaning fails, the original file is deleted. The file is not quarantined.
- Disinfect Yes / Delete No - An attempt is made to clean the original file. If cleaning fails the original file is moved to quarantine and the original file displays in the Security > View Threats page. If the original file is deleted using the View Threats page, both the quarantined copy and the original file are deleted.
- Disinfect No / Delete Yes - No attempt is made to clean the original file. The original file is deleted without putting a copy of the original file in quarantine.
- Disinfect No / Delete No - No attempt is made to clean or delete the file. The original file displays in the Security > View Threats page as infected.

Full Scan

The following types of files are considered 'infectable' 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 all files (except those excluded below) - If checked, all files are scanned for viruses on the managed machine.

Scan infectable files (filter by file content) - 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.

Scan infectable files (filter by extension type) - If selected, specifies the file extensions of programs and documents to include or exclude.

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.

Exclude files with these extensions - Specifies the file extensions of programs and documents to exclude from a scan. Applies to any of the three radio options above. Excluded extensions have precedence over included extensions. Enter each extension separated by a semi-colon (;) character.

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

Scan active processes - These are running applications. Applications can be normal software or virus/spyware/malware.

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

SCAN NTFS Alternate Data Streams - If checked, scanning includes alternate data streams. Each file in a NTFS volume can support alternate file names and alternate file data. Alternate data streams can hide data, especially rootkits, viruses, trojans, and other forms of malware.

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

Scan for spyware, adware, etc. - If checked, scanning includes spyware, adware, DLL-trojans, keyloggers and potentially unwanted programs.

Include cookies in spyware scan - If checked, scanning includes spyware cookies.

Include registry in spyware scan - If checked, scanning includes spyware entries in the registry.

Set priority of the scan to - Adjusts the priority of the scan against other tasks being performed on the managed machine.

- Do Not Set
- Low Priority
- Lower Priority
- Default Priority
- High Priority

Set a pause between files - If set to a value other than `None`, pauses after each file has been scanned for a specified time period. Pausing increases the performance of other tasks on the managed machine, but increases the time required to perform a full scan.

Once detected an infected file can be moved or deleted, but it cannot be opened, saved or copied. Use the following list to determine how to set the Disinfect and Delete checkboxes:

- Disinfect Yes / Delete Yes - An attempt is made to clean the original file. If cleaning fails, the original file is deleted. The file is not quarantined.
- Disinfect Yes / Delete No - An attempt is made to clean the original file. If cleaning fails the original file is moved to quarantine and the original file displays in the Security > View Threats page. If the original file is deleted using the View Threats page, both the quarantined copy and the original file are deleted.
- Disinfect No / Delete Yes - No attempt is made to clean the original file. The original file is deleted without putting a copy of the original file in quarantine.
- Disinfect No / Delete No - No attempt is made to clean or delete the file. The original file displays in the Security > View Threats page as infected.

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.

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 13)*.

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 11)* 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.

Check-in status

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

 Agent has checked in

 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

Machine ID.Group ID

The list of Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

Profile Name

Displays the security profile assigned to a machine ID.

Log Settings

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 11)* page.

Apply Configuration

Click Apply Configuration to apply the number of days specified in the Set 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 Set days to keep log entries field.

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 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

Machine ID.Group ID

The list of Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

Log Days Before Expiration

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

Updates

Security > Updates

The Updates page schedules updates machine IDs licensed to use Kaseya Endpoint Security with the latest version of security protection available.

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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 11)* page.

Update

Click Update to schedule an update of selected machine IDs using the update options previously selected.

Cancel Update

Click Cancel 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 Stagger by for 5 minutes, then the scan 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. If the machine is offline, skip and reschedule for the next day at the same 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.

Update from the Internet

Select Update from the Internet to download updates from the KServer.

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 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

Machine ID.Group ID

The list of Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

Last Scan

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

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 the machine ID.

Scheduled Time

Timestamp showing the next scheduled update. Indicates if the schedule is recurring.

Security Alarms

Security > Security Alarms

The Security Alarms page creates alarms in response to security protections events for 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 Kaseya Endpoint Security client software installed on the managed machine using the Security > Install/Remove *(page 11)* page.

To Create An Alarm

1. Check any of the following checkboxes to perform their corresponding actions when an alarm is triggered for a machine ID.
   - Create Alarm
   - Create Ticket
   - Run Script after alarm.
   - Email Recipients
2. Set additional email parameters.
3. Set security protection event checkboxes.
   - Virus Detected
   - Service Error
   - Protection Enabled
   - Definition Updated
   - Protection Disabled
   - Definition Not Updated For N Days
4. Check the machine IDs to apply the security alarm to.
5. Click the Add or Replace radio option.
6. Click Apply to assign security protection event triggers on selected machine IDs.

   A green checkmark displays for each security protection event selected in the VD PE PD SE DU DNU columns next to each selected machine ID.

To Cancel an Alarm

1. Select machine ID checkboxes.
2. Click Remove.

   All green checkmarks are removed from the VD PE PD SE DU DNU

columns next to each selected machine ID.

Passing Alarm Information to Emails and Scripts

The following variables are populated with information when an alarm is triggered. These variables can be referenced by any email you send or script you run in response to the triggering of an alarm.

Within an Email	Within a Script	Description
<at>	#at#	alert time
<ep>	#ep#	Kaseya Endpoint Security log message
<gr>	#gr#	group ID
<id>	#id#	machine ID
	#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

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.

Create Alarm

The Create Alarm check box is always checked.

Create Ticket

If checked, a new ticket is generated when an alarm is triggered.

Run Script after alarm

If checked, a script is run when an alarm is triggered. 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, emails are sent to the specified email addresses when an alarm is triggered.

- 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.

> Note: Changing this email format changes the format for *all security protection alarm* 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.

- If the Add to current list radio option is selected, when Apply is clicked alarm settings are applied and the specified email addresses are added to selected machine IDs without removing previously assigned email addresses.
- If the Replace list radio option is selected, when Apply is clicked alarm settings are applied and the specified email addresses replace the existing email addresses assigned to machine IDs.
- If Remove is clicked, all email addresses are removed from selected machine IDs without modifying any alarm parameters.
- 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.

Add / Replace

Select Add or Replace to add or replace security protection event triggers on selected machine IDs when the Apply button is clicked.

Remove

Click Remove to immediately remove security protection event triggers 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 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

Machine ID.Group ID

The list of Machine ID.Group IDs currently matching the Machine ID / Group ID filter.

Delete

Clicking the delete icon deletes security alarms for a machine ID.

Edit

Click a row's edit icon to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

ATSE

The ATSE alarm / 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.

VD PE PD SE DU DNU

If checked, triggers a security alarm for the following events:

- VD - Virus Detected
- PE - Service Error
- PD - Protection Enabled
- SE - Definition Updated
- DU - Protection Disabled
- DNU - Definition Not Updated For N Days

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 Deleted
- Threats Quarantined
- Threats
- Failed to Delete
- Threats Failed to Clean
- Threats Cleaned and Restored
- Threats Restored as is
- Scans Completed
- Updates Performed

The Network Health Score of the Executive Summary includes an Endpoint Score category. Untreated threats are the threats that have not yet been dispositioned using the Security > View Threats *(page 7)* 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.

Index