Kaseya Endpoint Security

User Guide

Version 1.2

March 11, 2008

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 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.

- 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.

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 7)*	Displays the current security status of machine IDs.
Updates *(page 5)*	Schedules updates of latest version of security protection definition files.
Schedule Scan *(page 7)*	Schedules security protection scans of machine IDs.
Enable/Disable *(page 8)*	Allows administrators to start or stop security protection of machine IDs.
View Threats *(page 9)*	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 24)*	Assigns security profiles to machine IDs.
Log Settings *(page 25)*	Specifies the number of days to keep security protection log data.
Install/Remove *(page 26)*	Installs or removes email protection for MS Exchange Server machines.
Define Alarm Sets *(page 29)*	Defines sets of alarm conditions used to trigger alerts using the Apply Alarm Sets page.
Apply Alarm Sets *(page 30)*	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 Display option to Enable/Disable Security Protection in Agent Icon Menu is checked in the General tab in Security > Define Profile *(page 17)*:

- 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 8)*.

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 and machine groups the administrator is authorized to see using System > Group Access. 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 14)* 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 Available Version

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

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 in. Tool tip lists the login 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.

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.

Email

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 30)*.

Manual Update

Security > Manual Update

The Updates page schedules 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 to review the update status of agents or to force an immediate update check if needed.

Note: Updating security protection cancels any in-process scans and executes the scans immediately after the update.

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 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 in. Tool tip lists the login 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.

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 KServer.

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.

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 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 in. Tool tip lists the login 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.

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 Display option to Enable/Disable Security Protection in Agent Icon Menu box in the General tab of 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 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:

- Enable - Click turn on security protection on selected machine IDs.
- Disable - Click 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 checked in and user is logged in. Tool tip lists the login 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.

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 the following 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.
- Add to PUP Exclusion List - Selected threats are added to the exclusion list for the profile assigned to the machine they were found on. The PUP Exclusion List is maintained using the Define Profile *(page 17)* > PUP Exclusions tab.
- Purge - Removes the threat record without taking any other action.

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.

Current / Historical

Click the Current Threats tab to display threats you can take action on. Click the Historical Threats tab to display threats you have already taken action on. For example, purged and deleted threats display only on the Historical Threats tab.

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.

Apply Filter / Reset Filter

Click Apply Filter to filter the rows displayed by the text entered in the Machine.Group, File Path or Threat Name fields. 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 display multiple records that match this expression.

- 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, Min, Max - Filter by a range of dates and times the threats were *last* detected.
- 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.
- Status - Filter by `Pending` or `Failed`. Displays only in the Current Threats page.

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 and machine groups the administrator is authorized to see using System > Group Access. 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 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. Types of security protection event codes include:

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

Apply Filter / Reset Filter

Click Apply Filter to filter the rows displayed by the text entered in the Time and Message fields. 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 display multiple records that match this expression.

- 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 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 an 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.

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 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 in. Tool tip lists the login 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.

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.

Licenses Used

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

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 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 checked in and user is logged in. Tool tip lists the login 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.

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 KServer.

Installed On

The date Kaseya Endpoint Security client software as 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 24)*. 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. Applies only to user-defined profiles.
- Save As - Creates a new security profile by saving it using a different name.
- Delete - Deletes an existing security profile. Applies only to user-defined profiles.
- Share - Shares a private security profile. Applies only to user-defined profiles. 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
   - Exchange
   - Exclude Dirs
   - Exclude PUPs
3. Click the Save or Save As button to save the security profile.

General

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, enables the Delete Files Older than <N> Days option.

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

Maximum Number of file to Store - Enter the maximum number of quarantined threats to store.

Display option to Enable/Disable Security Protection 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 > Enable/Disable *(page 8)*.

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

Delete and don't report tracking cookies - If checked, tracking cookies are deleted automatically.

Note: Checking this option is recommended, because it removes many rows of data from the View Threats *(page 9)* page.

Resident Protect

Resident protect is a memory-resident feature.

Enable Resident 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; 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 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.

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.

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 File Close - 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.

Email Protection

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

> Note: This email protection applies to local email clients, such as Outlook, installed on the managed machine. It does not apply to email protection for MS Exchange Servers

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 Mail - If selected, incoming email is not certified.

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

Only Certify Mail with Attachments - If selected, only incoming email with attachments are certified.

Incoming Mail Certification - Certification text appended to incoming email.

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.

Only Certify Mail with Attachments - If selected, only outgoing email with attachments are certified.

Outgoing Mail 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 Heuristic Analysis - 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.

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

Scan Attached Archives (RAR, RAR 3.0, ZIP, ARJ, CAB) - 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 9)* page.

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

Remove Attachments - If checked, remove all executable files or documents, whether infected or not, from the email.

Remove All Executable Files - If checked, executables files, whether infected or not, are removed from email.

Remove All Documents - If checked, documents, 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

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

Scan Active Processes for Viruses - 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 All Files Except Those Identified In Exceptions - If checked, all files are scanned for viruses on the managed machine.

Scan infectible files - 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

Add Extensions - Specifies the file extensions of programs and documents to include in a scan. Enter each extension separated by a semi-colon (;) character.

Use Smart Scan - Recognizes the file type regardless of its extension. Applies only if Scan infectible Files is selected.

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

Enable Anti-Spyware - If checked, scanning includes spyware, adware, DLL-trojans, keyloggers and potentially unwanted programs.

Enable Cookie Detection - If checked, scanning includes spyware cookies.

Enable Registry Detection - If checked, scanning includes spyware entries in the registry.

Select System Priority to Scan - 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

Gaps During file Scan - 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.

Exchange: Product

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 (e.g. e-mail 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 - 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.

Move Files to Quarantine - If checked, infected e-mail messages are moved into quarantine.

Delete infected messages (Exchange Server 2003 only) - If checked, messages with viruses are deleted. If blank, infected email is delivered to recipients, but infected attachment is replaced with a text file containing information on the virus detected. This option is available only in VSAPI 2.5 in Exchange 2003 Server.

> Note: The Microsoft Exchange Virus Scan API (VSAPI) provides a way for anti-virus software to scan at a very low-level in the Exchange store. This allows a virus scanning application to run with high performance and guarantees that the message will be scanned before any client can access a message or attachment.

Exchange: Plugin

These attributes determine how email protection is applied to MS Exchange Servers. See Email Protection for local email clients above for a description of each attribute.

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).

> Warning: Do not exclude files unless the contents of the files 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 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 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.

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 in. Tool tip lists the login 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.

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 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 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.

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 in. Tool tip lists the login 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.

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.

MS Exchange Server email protection license are purchased separately from Kaseya Endpoint Security exchange server licenses. Each email account consumes *one license each day* that email protection is applied to the MS Exchange Server. MS Exchange Server licenses are allocated by group and

sub-group using System > License Manager.

> 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 9)* 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 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.
- 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.

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.

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.

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 in. Tool tip lists the login 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.

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 KServer.

Mailboxes

The number of email accounts on the MS Exchange Server.

Installed On

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

Define Alarm Sets

Security > Define Alarm Sets

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

The page provides you with the following actions:

- Save - Save and 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 <Select an Alarm Set> 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. 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.

Alarm Conditions

Check any of the following types of alarm conditions to include it in an alarm set:

- Threat Detected (Virus)
- Threat Detected (Spyware)
- Threat Detected (Unknown)
- Protection Enabled
- Protection Disabled
- Service Error
- Definition Updated
- Definition Not Updated in <N> days
- Threat Cleaned
- Threat Moved To Quarantine
- Threat Deleted
- Threat Restored

- Threat Clean Failed
- Threat Move To Quarantine Failed
- Threat Delete Failed
- Threat Restore Failed
- Scheduled Scan Completed
- Scheduled 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 29)*. 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 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 machine ID encounters an alarm condition.
   - 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>	#db-view/column#	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#	KES alarm
<st>	#st#	KES alarm specific title
<tk>	#tk#	ticket ID
<ty>	#ty#	KES 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.

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 in. Tool tip lists the login 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.

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.

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 have not yet been dispositioned using the Security > View Threats *(page 9)* 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.

Chapter 2

Notices

In This Chapter

Third Party Software Notices and/or Terms and Conditions

The following are Third Party Software Notices and/or Terms and Conditions for licensed third party software components included within Kaseya products.

RSS.NET

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Rhino Tools

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Ayende Rahien nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE

COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index