

# **eTrust<sup>®</sup> Antivirus Groupware Options**

## **User Guide**

r8



Computer Associates®

This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been destroyed.

To the extent permitted by applicable law, CA provides this documentation "as is" without warranty of any kind, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or noninfringement. In no event will CA be liable to the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

© 2005 Computer Associates International, Inc.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

# Contents

---

<b>Chapter 1: Understanding Messaging/Groupware Systems</b>	<b>7</b>
Protecting Your Network and the Messaging System.....	8
Groupware Options .....	8
Exchange Option Features .....	9
Notes Option Features.....	10
<b>Chapter 2: Installing the Exchange Option</b>	<b>11</b>
Customizable Installation Using an ICF File .....	11
Install the Microsoft Exchange Option.....	12
Test Your Installation.....	12
<b>Chapter 3: Installing the Notes Option</b>	<b>13</b>
Install the Lotus Notes/Domino Option .....	13
Test Your Installation.....	14
<b>Chapter 4: Common Features of Groupware</b>	<b>15</b>
Realtime Scans .....	15
Local Scans.....	15
Scheduled Scans .....	16
Mail Scanner .....	16
Exchange Option Mail Scanner.....	17
Notes Option Mail Scanner .....	18
Quarantine Folder .....	19
Show Last Scan Summary.....	19
Log Viewer .....	19
<b>Chapter 5: Setting Exchange Options</b>	<b>21</b>
Realtime Scanning .....	21
Access the Realtime Mail Options Dialog.....	21
Scan Tab.....	22
Selection Tab.....	25
Notification Tab.....	31
Options Tab.....	33
Misc Tab.....	34
Statistics Tab .....	35

---

Local Scanning .....	35
Access the Email Options Dialog .....	35
Options Tab .....	36
Log Tab.....	36
Scheduled Scanning .....	37
Access the Scheduled Scan Job Options Dialog.....	37
Description Tab .....	37
Options Tab .....	37
Schedule Tab .....	38
Include Mailboxes Tab .....	38
Exclude Mailboxes Tab.....	39
Scheduled Job Statistics Dialog.....	39
Detailed Result For Dialog .....	40
Scan Result Summary Dialog .....	41
Logging .....	41
Purge Logs Dialog.....	42
Customizable Warning Messages .....	42
Sample MRTCONFIG.INI .....	43

## **Chapter 6: Setting Notes Options 45**

Realtime Scanning .....	45
Access the Realtime Mail Options Dialog.....	45
Scan Tab.....	46
Selection Tab .....	49
Notification Tab .....	54
Statistics Tab .....	55
Local Scanning .....	56
Access the Email Options Dialog .....	56
Scan Tab.....	57
Selection Tab .....	60
Options Tab .....	64
Log Tab.....	64
Notification Tab .....	65
Scheduled Scanning .....	66
Access the Scheduled Scan Job Options Dialog.....	66
Description Tab .....	67
Scan Tab.....	68
Selection Tab .....	71
Options Tab .....	75
Schedule Tab .....	76
Include Directories Tab.....	77
Exclude Directories Tab .....	78

---

Notification Tab .....	79
Scheduled Job Statistics Dialog.....	80
Detailed Result For Dialog .....	81
Scan Result Summary Dialog .....	82
Mail Scanner Folders.....	82
Add Folder Dialog .....	83
Logging .....	83
Purge Logs Dialog.....	83
Customizable Warning Messages .....	84
Sample NOTESSTR.INI .....	85
<b>Index</b>	<b>89</b>



# Chapter 1: Understanding Messaging/Groupware Systems

---

Using an electronic messaging system is a common way for today's corporations to communicate. Quite often, the messaging system becomes an essential method for sharing information and documents, both within and outside of the enterprise. Unfortunately, these same systems can have gaps in security that enable infections to rapidly spread through an organization—posing risks to both data and productivity.

According to an International Computer Security Association (ICSA®) survey, email attachments are the most common sources of infections. Macro viruses, worms, and other malicious code can come in through email to slow down and debilitate your system. For example, infectors such as the Winword Concept macro virus and the Melissa virus have become among the fastest spreading viruses in history. According to the ICSA, the well-known LoveLetter virus is a mass-mailer, and therefore has the potential to spread quickly. The virus arrives as a VBS file attached to an email message.

A 1996 ICSA survey states that macro viruses comprise 49 percent of all viruses detected. Until the Winword Concept virus was born, most viruses lived in and infected only executable regions of magnetic media (like boot sectors) and files (like .EXE, .COM, .BIN, and so on). Now macro viruses have become a common method of delivering infectors. Macro viruses can inhabit and attach themselves to the NORMAL.DOT template of Microsoft Word files on Windows operating systems. Other types of damaging infectors have also become widespread, and variations appear all the time.

Messaging systems pose a special problem for antivirus products because files are stored in a database format, not in a normal file system. No antivirus product can scan such systems by itself. However, eTrust Antivirus can protect users from viruses when documents are detached from messages and saved to the hard drive. It has the unique ability to penetrate the database barrier, and completely scan and cure server-based messaging systems. As a result, macro viruses and other malicious infected files need no longer pose a threat to your company's messaging/database system.

## Protecting Your Network and the Messaging System

There are several things you can do to ensure that your system and the rest of your network are fully protected against the latest infections:

- Download the latest signature files as soon as eTrust Antivirus and the groupware option are installed. Computer Associates always detects new infections and updates the signature files, so it is best to make sure you have the latest protection technology.
- Set all of your executable files as Read-Only files. This reduces the chance of executable files becoming infected.
- Scan floppy disks for infections before you copy any files from them.
- Use a backup tool that is compatible with your system, such as Computer Associates BrightStor, to back up your workstation after you successfully scan it for infections. This way, if a file is detected with an infection that cannot be cured, you can restore a backed up version of that file.
- Check the Computer Associates SupportConnect website (<http://supportconnect.ca.com/>) regularly.
- Subscribe to the free Computer Associates online antivirus newsletter for information about the latest viruses.

## Groupware Options

There are two messaging/groupware systems supported by eTrust Antivirus: Microsoft® Exchange and Lotus Notes/Domino. When the appropriate option is installed, you can scan your mail databases and directories for infections. Install one of the following options on your organization's mail server:

- eTrust Antivirus Option for Microsoft Exchange Option (also referred as the Exchange Option)
- eTrust Antivirus Lotus Notes Domino Option (also referred to as the Notes Option)

## Exchange Option Features

Some important features of the Exchange Option include the following:

### **Mail Scanning**

Detects and processes any infected files sent through Microsoft Exchange mail. Realtime protection is automatic and continuous. You can also perform immediate and scheduled scans on demand.

### **Macro Virus Analyzer**

Detects and completely removes macro viruses, which are capable of spreading very rapidly. Documents attached to emails are automatically detached and examined. They are reattached automatically if found to be clean or if the infected attachments can be cured.

### **Live Scanning**

Scans for viruses while messaging systems are live and running, transparent to end users.

### **Easy-to-use Options**

Lets you easily specify detection, alerting, and log options, such as curing infected files, alerting the system administrator, and setting the detail level of logs.

### **Notification**

Sends virus notifications to the person whose inbox received the infected email, the person who sent the infected email, or the Microsoft Exchange administrator. You can also attach the notifications directly to the email containing the virus.

## Notes Option Features

Some important features of the Notes Option include the following:

### **Mail Scanning**

Detects and processes any infected files sent through Lotus Notes mail. Realtime protection is automatic and continuous. You can also perform immediate and scheduled scans on demand.

### **Macro Virus Analyzer**

Detects and completely removes macro viruses, which are capable of spreading very rapidly. Documents attached to emails are automatically detached and examined. They are reattached automatically if found to be clean or if the infected attachments can be cured.

### **Live Scanning**

Scans for viruses while messaging systems are live and running, transparent to end users.

### **Easy-to-use Options**

Lets you easily specify detection, alerting, and log options, such as curing infected files, alerting the system administrator, and setting the detail level of logs.

### **Notification**

Sends virus notifications to the person whose inbox received the infected email, the person who sent the infected email, or the Lotus Notes administrator. You can also attach the notifications directly to the email containing the virus.

# Chapter 2: Installing the Exchange Option

---

The Exchange Option integrates with eTrust Antivirus to scan for infections in documents attached to email messages and folders. Use this option, to automatically cure infected Microsoft Exchange attachments. The Exchange Option scans all mail passing through the server.

The Exchange Option runs on the server where the Microsoft Exchange Server resides. It can detect, cure, or block infected email attachments and prevent them from spreading throughout your enterprise.

Before you install the Exchange Option, review the Readme file to verify that you have the required software and hardware. You must also ensure that your Microsoft Exchange account has its user rights configured properly and meet the Exchange Full Administrator requirement.

## Customizable Installation Using an ICF File

You can use the INXSETUP.ICF file to configure the Exchange Option installation and the default realtime settings before you install the product. By configuring the settings in advance, one image can be applied to multiple computers with the assurance that the realtime policies at installation time are the same across all computers.

The sample INXSETUP.ICF file is included on the product media. See this file for a description of the configuration settings and options available. If you choose to run the installation program silently from a shared drive or a batch program, all of the configuration settings are taken from the INXSETUP.ICF file. You can run setup silently using the following command:

```
SETUP /s.
```

## Install the Microsoft Exchange Option

First, complete the installation of eTrust Antivirus.

To install the Microsoft Exchange Option on your Microsoft Exchange Server, follow these steps:

1. Insert the product media into the drive.
2. When the installation screen appears, select the Microsoft Exchange installation option.
3. Follow the instructions in the setup wizard to complete the installation.

## Test Your Installation

You can use the EICAR test standard to test the installation of your Exchange Option. The EICAR standard has been developed by the European Institute for Computer Antivirus Research to create a benign email attachment that is detected as an infected file.

To test your installation, follow these steps:

1. Copy the following line into a text file:

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

The above sample code is for the EICAR Standard Antivirus Test File.

2. Save the text file with the name EICAR.COM. The file should be approximately 69 or 70 bytes in size.
3. Attach the EICAR.COM file to a test Microsoft Exchange email. If the installation was successful, eTrust Antivirus detects the attachment and takes the appropriate treatment action on it:
  - If you chose to quarantine, delete, or block the attachment, it is replaced with AV-SCANREPORT.TXT.
  - If you chose to report, rename, or cure the attachment, a ZIP archive file is created that contains both AV-SCANREPORT.TXT and the original attachment with its treatment applied.
4. After conducting the test, delete the EICAR.COM file.

# Chapter 3: Installing the Notes Option

---

The Notes Option integrates with eTrust Antivirus to scan for infections in documents and email file attachments. Infected Lotus Notes attachments can be automatically detected. This option also notifies the users through the host messaging system whenever an infection is found.

Before you install the Notes Option, review the Readme file to verify that you have the required software and hardware. You must also ensure that your Lotus Notes Domino account has its user rights configured properly.

## Install the Lotus Notes/Domino Option

First, complete the installation of eTrust Antivirus.

To install the Lotus Notes/Domino Option on your Lotus Notes/Domino Server, follow these steps:

1. Insert the product media into the drive.
2. When the installation screen appears, select the Lotus Notes installation option.
3. Follow the instructions in the setup wizard to complete the installation.

## Test Your Installation

You can use the EICAR test standard to test the installation of your Notes Option. The EICAR standard has been developed by the European Institute for Computer Antivirus Research to create a benign email attachment that is detected as an infected file.

To test your installation, follow these steps:

1. Copy the following line into a text file:

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

The above sample code is for the EICAR Standard Antivirus Test File.

2. Save the text file with the name EICAR.COM. The file should be approximately 69 or 70 bytes in size.
3. Attach the EICAR.COM file to a test Lotus Notes email. If the installation was successful, eTrust Antivirus detects the attachment, takes the appropriate treatment action on it, and then attaches the scan result file, eTrust Antivirus Scan Report.TXT, to the email.
4. After conducting the test, delete the EICAR.COM file.

# Chapter 4: Common Features of Groupware

---

This section describes the various views available for groupware options and how to perform basic actions using these views.

## Realtime Scans

The key to a secure enterprise is realtime scanning. Realtime scanning catches infections as users try to send them to other users, which prevents the spread of infections.

The Exchange Option can be configured to scan any existing Microsoft Exchange database files and mailboxes for malicious code. All email scanned with the Exchange Option passes through the realtime scanner, even when a local scan or scheduled scan is run.

The Notes Option can be configured to scan any existing Lotus Notes/Domino database files for malicious code. As a server-based mail system, all emails in the Notes Option pass through the Computer Associates antivirus mailbox before they are sent to the Lotus Notes/Domino server. eTrust Antivirus sets up a barrier on the server that catches infections coming in—preventing both the server and the end users from being infected.

## Local Scans

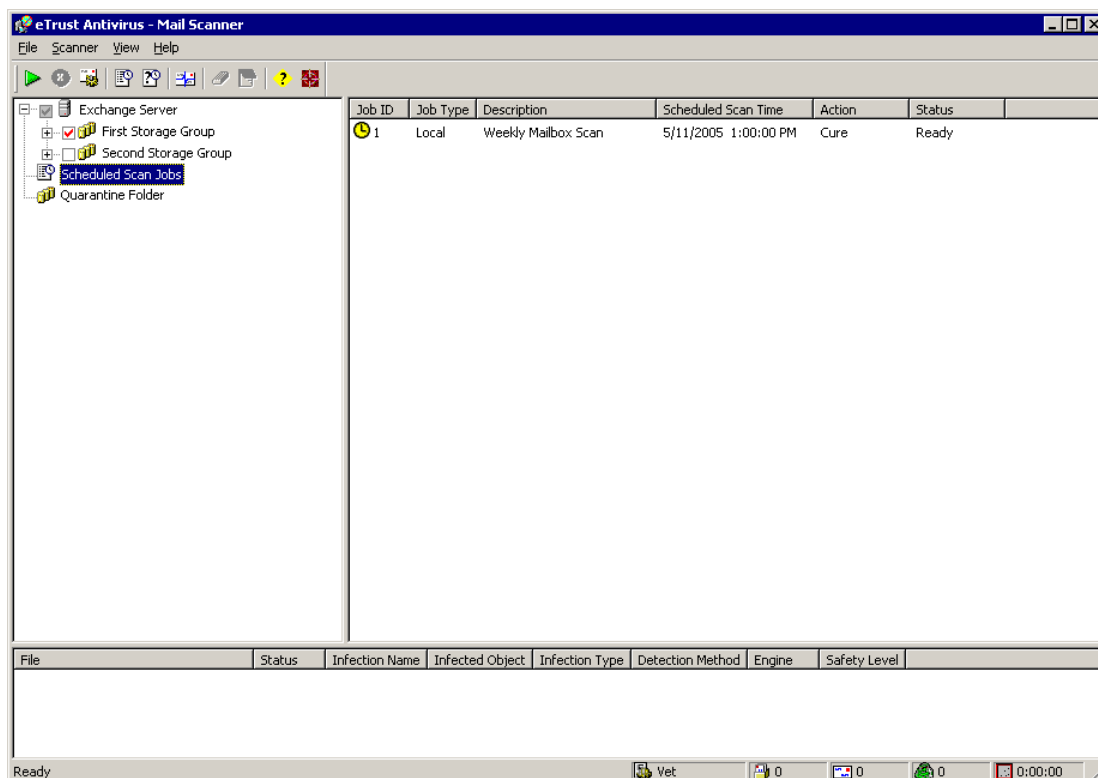
For a local scan with the Exchange Option, you select the appropriate subset of databases to scan. You can specify particular mailboxes or just scan all mailboxes one or more parent databases.

For a local scan with the Notes Option, you select the appropriate subset of directories to scan. You can specify particular database files in those directories or just scan all databases in one or more directories.

You can configure various settings for how local scans should run.

## Scheduled Scans

The Mail Scanner window with the Scheduled Scan Jobs category selected in the left pane appears as follows:



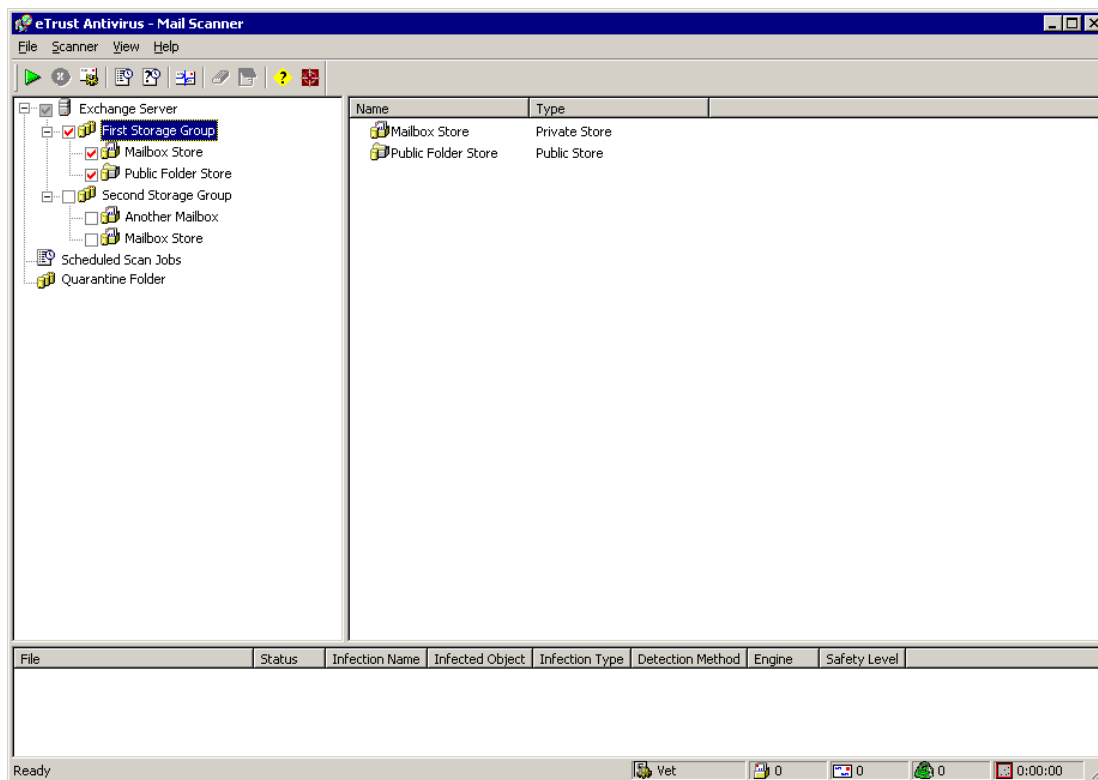
Statistics for scheduled scans are available, while they run, in the Scheduled Job Statistics dialog. New scheduled scan jobs are created using the Scheduled Scan Job Options dialog. You can edit an existing scheduled scan job by highlighting it, right-clicking, and choosing Options from the pop-up menu. You can delete a scheduled scan job by right-clicking and choosing Delete.

## Mail Scanner

The Mail Scanner window is the window that enables you to manage all your groupware system scanning activities. You can perform a manual local scan of your mailboxes, databases, or directories, depending on which groupware system is in use. You can schedule scans or modify any of your scan settings from this window. The window displays differently depending on your groupware system.


## Exchange Option Mail Scanner

The Mail Scanner view for the Exchange Option appears as follows:



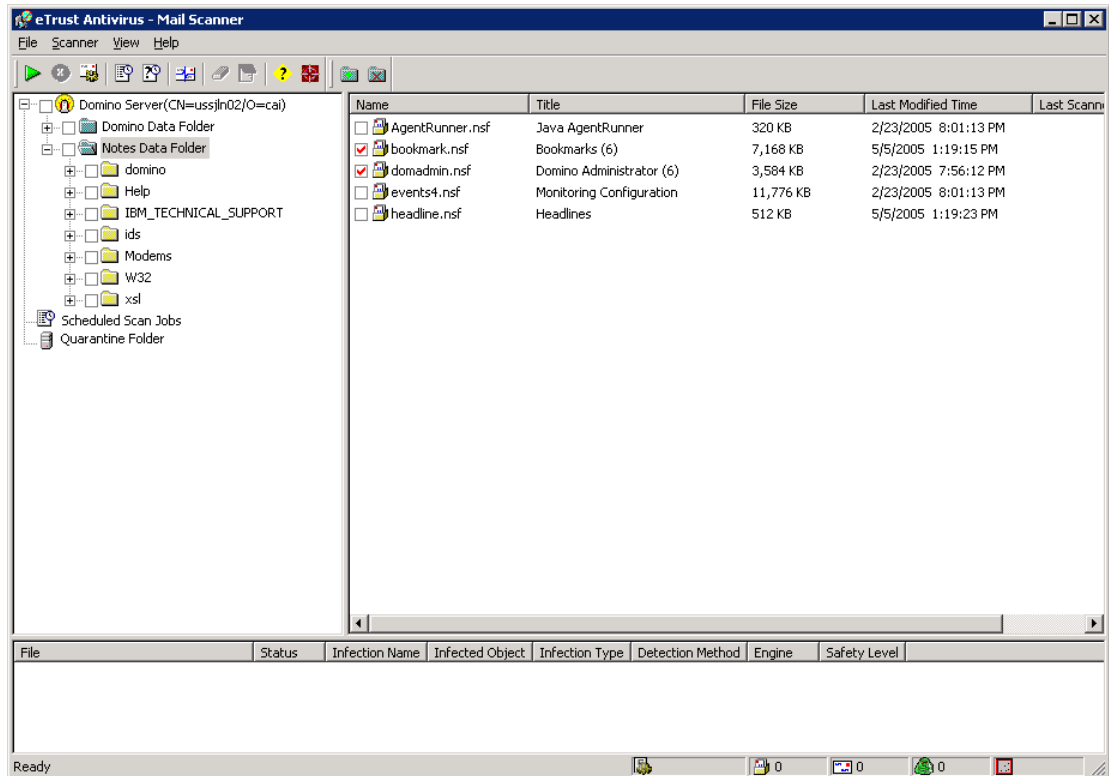
Three categories appear in the left pane: Exchange Server, Scheduled Scan Jobs, and Quarantine Folder. Exchange Server has a plus sign next to it to indicate that it can be expanded into a tree view.

For a local scan, select the appropriate subset of databases by expanding the branches of the tree under Exchange Server. The individual mailboxes for the highlighted branch display in the right pane with check boxes next to them. You may select and clear these to specify the mailboxes you want to scan, or select one or more entire databases in the left pane.

When you are finished, click the  icon on the toolbar to initiate the scan. Upon completion of the scan, eTrust Antivirus displays a summary of scan results in a dialog and any infected mail files display in the bottom pane of the Mail Scanner window. If you double-click an infected file, a dialog appears, showing detail information for that file.


## Notes Option Mail Scanner

The Mail Scanner view for the Notes Option appears as follows:



Three categories appear in the left pane: Domino Server, Scheduled Scan Jobs, and Quarantine Folder. Domino Server has a plus sign next to it to indicate that it can be expanded into a tree view.

For a local scan, select the appropriate subset of directories in the left pane by expanding the branches of the tree under Domino Server. The individual database files for the highlighted branch display in the right pane with check boxes next to them. You may select and clear these to specify the databases you want to scan, or select one or more entire directories in the left pane.


When you are finished, click the  icon on the toolbar to initiate the scan. Upon completion of the scan, eTrust Antivirus displays a summary of scan results in a dialog and any infected database files display in the bottom pane of the Mail Scanner window. If you double-click an infected file, a dialog appears, showing detail information for that file.

**Note:** You may also add additional data folders by highlighting Domino Server, right-clicking, and selecting Add Favorite Folder.

## Quarantine Folder

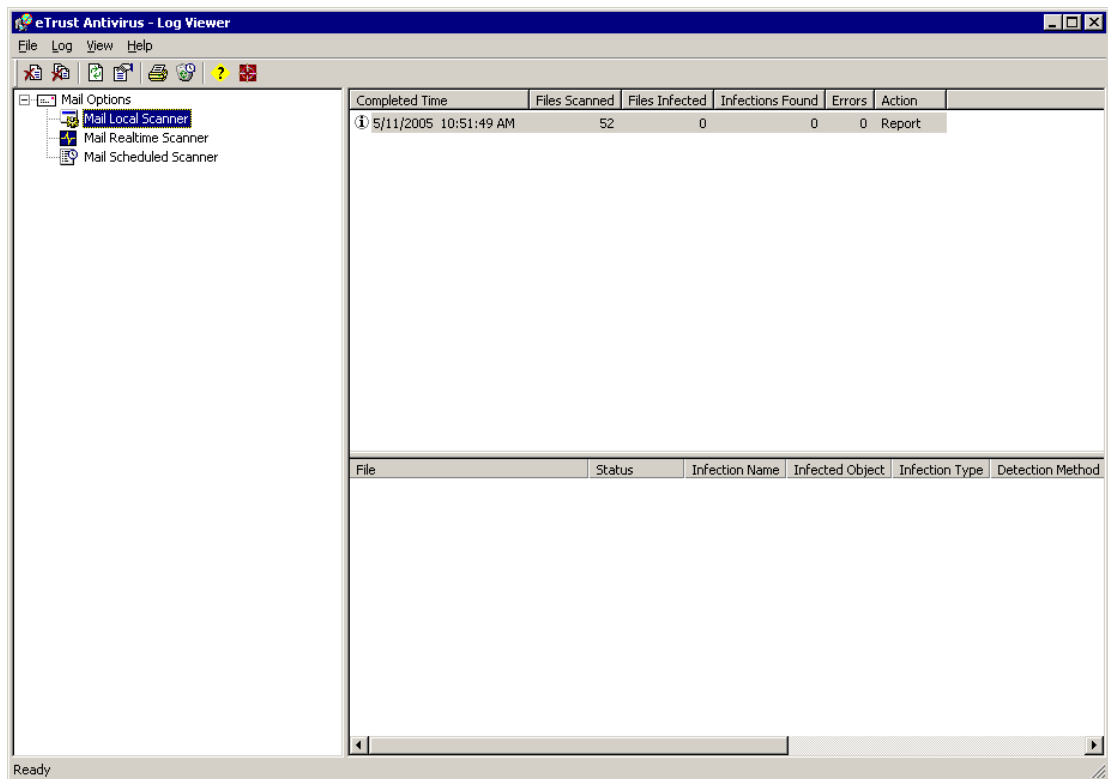
Select the Quarantine Folder category in the left pane to display information in the right pane about attachments from mail and database files that are infected and quarantined.

## Show Last Scan Summary

To display the scan results summary for the most recent scan performed, click the  icon on the toolbar. This displays summary statistics about the scan.


## Log Viewer

The Log Viewer view appears as follows:



You can view past scan results for any of the three types of scans by clicking the appropriate one in the left pane. To view detail for a specific log, highlight it. Any infected mail files for that scan job display in the bottom pane.

You can print one or more logs by highlighting the ones you want to print, right-clicking, and choosing Print Log(s) from the pop-up menu. You can view the properties of the scan job associated with this log by right-clicking and choosing Property. You can delete a log by right-clicking and choosing Delete.

To access purge options for your logs, click the  icon. This opens the Purge Logs dialog.

# Chapter 5: Setting Exchange Options

---


This chapter describes the features specific to the Exchange Option, and how to guard your system from infections in emails or in your mailbox database.

For more information about managing email options from the administrator console of eTrust Antivirus, see the *eTrust Antivirus Administrator Guide*.

## Realtime Scanning

The Exchange Option supports realtime scanning and setting changes through the Realtime option in the system tray. The Realtime Mail Options dialog has six tabs for managing realtime email scans.

### Access the Realtime Mail Options Dialog

To access the Realtime Mail Options dialog, click the  icon on the toolbar.

Alternately, right-click the Realtime Monitor icon in the system tray and choose Mail Options from the pop-up menu.

## Scan Tab

Use the Scan tab to choose your scanning engine, specify a safety level, and perform file actions.

This tab contains the following fields:

### **Incoming and Outgoing Messages**

Enables realtime scanning by the email option. If this option is disabled, there is no email protection.

### **Scanning Engine**

Lets you choose the scanning engine to use, if a choice is available. The scanning engine is the specialized processor that does the work of looking for infections. The installation process automatically selects the appropriate scanning engine for your configuration. Most users do not need to change this option. It is primarily for advanced corporate users at large enterprises. The following engines may be available:

#### **InoculateIT**

Specifies the base eTrust Antivirus scanning module typically used.

#### **Vet**

Specifies an alternative scanning module.

### **Heuristic Scanner**

Includes the Heuristic Scan engine in realtime scanning. The Heuristic Scan engine scans for infections whose signatures have not yet been isolated or documented.

### **Specify how thorough the scan should be**

You can set the scan safety level to Secure or Reviewer mode. Use the Secure mode as the standard method for scanning files completely.

If you suspect you have an infection that is not being detected by the Secure mode, you can use the Reviewer mode. The Reviewer mode is used to detect a virus that is inactive or deliberately modified, such as in a virus testing laboratory. In addition, Reviewer mode runs significantly slower than Secure mode.

**Note:** In unique circumstances, Reviewer mode can generate a false alarm. Therefore, if you are using this mode as your standard scanning option, use it with the Report Only option.

### **File Actions**

Indicates how to treat the infection. The following infected file actions are available:

**Report Only**

Reports when an infection is found. If you want to know if there are any infections before you decide what to do with an infected file, choose the Report Only infection treatment. If an infection is found, you can then choose any of the other available treatments.

**Delete File**

Deletes an infected file.

**Rename File**

Renames an infected file with an AVB extension. Infected files with the same name are given incremental extensions in the form #.AVB (for example, FILE.0.AVB, FILE.1.AVB, and so on). After a file is renamed with an AVB extension, it is not scanned subsequently.

**Quarantine File**

Moves an infected file from its current directory to the Quarantine folder.

**Cure File**

Attempts to cure an infected file automatically. Even if the infected file is cured, it is recommended that you delete the infected file and then restore the original file from a backup. If the infected file is from a software package, restore the file from the product installation disks.

This tab contains the following unique button:

**Cure Options**

Opens the Cure Action Options dialog so you can specify how to cure the file. This button is only available if Cure File was chosen as your infection treatment.

## Cure Action Options Dialog

Use the Cure Action Options dialog to specify how to deal with macro viruses and Trojan infections, and what actions to perform before or after a cure is attempted.

This dialog contains the following fields:

### **Copy File**

Copies the file to the Quarantine folder before the cure is attempted.

### **Action to perform if cure fails**

Indicates the actions to perform if a cure fails. The following actions are available:

#### **No action**

Leaves the infected file as is.

#### **Quarantine file**

Moves the infected file into the Quarantine folder.

#### **Rename file**

Renames the infected file with an AVB extension.

### **Cure by Deleting**

Deletes the infected file when a Trojan or Worm infection is found.

### **Macro viruses treatment**

Indicates how to treat macro viruses. The following methods are available:

#### **Remove infected macros**

Removes only infected macros from the file.

#### **Remove all macros**

Removes all macros from the file.

## Selection Tab

Use the Selection tab to choose types of file extensions to include or exclude from a scan and types of compressed files to scan.

This tab contains the following fields:

### **Regular Files**

Indicates what subset of file extensions to scan. Each option has its own list of default extensions. The following subsets are available:

#### **All Extensions**

Scans files with all types of extensions.

#### **Specified Extensions Only**

Scans files with the specified file extensions only.

#### **All Except the Specified Extensions**

Scans files with all types of extensions except those specified.

### **Scan Compressed Files**

Enables you to scan compressed files. Select the Scan Compressed Files check box and then indicate the extensions for the types of compressed files.

This tab contains the following unique buttons:

#### **Edit List**

Depending on your selection for Regular Files, opens either the Specified Extensions Only dialog or the All Except the Specified Extensions dialog to let you add or remove file extensions for scanning.

#### **Options**

Opens the Compressed File Options dialog, where you can specify additional management information for compressed files.

#### **Choose Type**

Opens the Compressed File Type dialog, where you can select the compressed file types to allow in a scan.

#### **Block**

Opens the Block Extension List dialog, where you can specify file extensions to block from the scan.

#### **Exempt**

Opens the Exempt From Blocking dialog, where you can specify particular files to include in the scan even though their extensions are blocked.

## Specified Extensions Only Dialog

Use the Specified Extensions Only dialog to specify file extensions to include in a regular file scan.

This dialog contains the following fields:

### **Enter a new file extension**

Indicates the file extension to add to the list of file extensions.

### **List of File Extensions**

Displays the current file extensions selected. Extensions can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file extension specified in the Enter a new file extension field to the list.

### **Remove**

Removes one or more file extensions from the list. To specify the appropriate extensions, select the check boxes to their left.

## All Except the Specified Extensions Dialog

Use the All Except the Specified Extensions dialog to specify file extensions to exclude from the regular file scan.

This dialog contains the following fields:

### **Enter a new file extension**

Indicates the file extension to add to the list of file extensions.

### **List of File Extensions**

Displays the current file extensions selected. Extensions can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file extension specified in the Enter a new file extension field to the list.

### **Remove**

Removes one or more file extensions from the list. To specify the appropriate extensions, select the check boxes to their left.

## Compressed File Options Dialog

Use the Compressed File Options dialog to set additional options managing compressed files. These can be used to improve scan performance.

This dialog contains the following fields:

### **Apply extension filter to files inside archives**

Scans compressed files based on the list of regular files selected on the Selection subtab.

### **Stop scanning archive when an infected file is found**

Stops scanning the compressed file archive when an infected file is found in it.

### **Apply infection actions to archives**

Applies specified infection treatment options, other than Cure File, to compressed files in the archive.

### **The file's Extension (faster)**

Scans compressed files by recognizing them by extension, which is faster than analyzing them by the contents of the archive.

### **The file's Contents (slower)**

Scans compressed files by analyzing the contents, which is slower than recognizing them by extension.

## Compressed File Type Dialog

Use the Compressed File Type dialog to indicate which compressed file types to include in your scan. The compressed file types that are currently supported for scanning include:

- ARJ
- GZIP
- LHA
- Microsoft cabinet file
- Microsoft compressed file
- MIME
- ZIP or Java archive
- RAR
- UNIX compressed file (.Z)
- TNEF encapsulated eMail files
- TAR
- CA Zip
- BZIP
- self extracting archive

This dialog contains the following fields:

### **File types**

Lets you compile a list of compressed file types that you want the scanner to include. Select and clear the appropriate check boxes.

### **Common file extensions for the selected type**

Displays all applicable extensions for the file type to which you are currently pointing, such as CAB for Microsoft cabinet file.

## Block File List Dialog

Use the Block File List dialog to specify files to block. When a file is blocked, that file is not scanned and all access to the file is denied. For example, if FILENAME.EXT is entered, only attachments with FILENAME.EXT and no other variations are blocked. The blocking mechanism is case insensitive.

**Note:** To block file extensions or file name endings, you can use a wildcard. For example, if you want to block all files with the EXE extension, enter the following: \*.EXE.

This dialog contains the following fields:

**Enter a new file name here**

Indicates the file to add to the list of blocked files.

**List of file names**

Displays the current files selected for blocking. Files can be added or removed.

This dialog contains the following unique buttons:

**Add**

Adds the file or file extension specified in the Enter a new file name here field to the list.

**Remove**

Removes the selected file or file extension from the list.

## Exempt from Blocking Dialog

Use the Exempt from Blocking dialog to include one or more files in realtime scanning even though the associated file extension is included in the pre-scan block list.

This dialog contains the following fields:

### **Enter an email attachment's file name**

Indicates the file name of the email attachment to add to the list of exempt files. These files are scanned and then delivered even if their extensions are specified in the blocked list.

### **List of Exempt Files**

Displays the current files selected for exemption. Files can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file specified in the field to the list.

### **Remove**

Removes the selected file from the list.

## Notification Tab

Use the Notification tab to configure who is to be notified of the infection and the subject of the notification. By default, the recipient is always notified. Other than the recipient, the notification only includes information about the infection and never the infected attachment or email.

This tab contains the following fields:

### **Notify Mailbox Owner**

Indicates whether to notify the person who received the mail that an infection was attached. This check box is always selected and cannot be modified.

### **Notify Message Sender**

Indicates whether to notify the user who sent the infected mail or created the database containing the infection. By using this option, you can track the infected file to its origin, and notify the owner of the mailbox that originally mailed the infected file.

### **Notify Mail System Administrators**

Indicates whether to notify specified system administrators that network security might have been violated. The administrators can then take whatever actions are needed to secure the network.

### **Send scan results to generate reports**

Indicates whether the scan results should be forwarded, allowing them to be used to generate reports.

### **Return to address**

Indicates where to reroute a notification if it is undeliverable to the original address.

### **Default Subject**

Specifies the subject for the notification.

This tab contains the following unique button:

### **Administrators**

Opens the Notify Administrators dialog so you can enter a list of administrators to notify with security issues.

## Notify Administrators Dialog

Use the Notify Administrators dialog to specify administrators to contact when there is a mail-related security concern.

This dialog contains the following fields:

### **Enter an email address**

Specifies the email address at which to contact the administrator.

### **List of administrators**

Lists the administrators that are notified when there is a security concern.

This dialog contains the following unique buttons:

### **Add**

Adds the email address in the Enter an email address field to the List of administrators box.

### **Remove**

Removes the highlighted email address from the List of administrators box.

## Options Tab

Use the Options tab to choose custom settings for scanning email on your Microsoft Exchange server. You can select from among the available options to fine tune the performance of eTrust Antivirus on your Microsoft Exchange server.

This tab contains the following fields:

### **Scan Message Body**

Indicates whether to scan the body of email messages.

### **Proactive Scanning**

Indicates whether to enable Microsoft scan queue prioritization. If you disable proactive scanning, items are only scanned when they are accessed directly by a user or by the on-demand scanner, or scanned by a background scanning thread.

### **Scanning Threads**

Lets you specify the number of threads in the global thread pool. Note that when you increase the number of scanning threads, you can adversely affect the performance of your system. The default value is recommended by Microsoft.

### **Scan Timeout**

Lets you specify the timeout value, in seconds. You can specify a timeout value to increase timeout on a heavily loaded system.

## Misc Tab

Use the Misc tab to specify a variety of miscellaneous options. Use the Log options to specify the log size, number of logs to keep, and the detail level of the log. You can also activate the System Event Log, specify the timeout value, and enable background scanning from this tab.

This tab contains the following fields:

### Specify the log size

Lets you specify the desired log size, in megabytes.

### Specify the number of logs to keep

Lets you select the number of logs you want to keep. The logs are stored in the antivirus installation directory, using the format InXScan####.log or StoreVS(2)####.log (where #### represents 0000, 0001, and so on).

### Specify the detail level of the log(s)

Indicates the log detail level as follows:

- 0 = No logging
- 1 = Only log infected files
- 2 = Log all scanned files

### System Event Log

Enables the email option to create an event in the application event log when it finds an infected attachment.

**Note:** If this option is turned on and there is a virus attack, the application event log will fill up quickly.

### Specify the timeout value

Specifies the maximum amount of time (in seconds) a thread can wait for scanning to be completed. If scanning is not completed before the timeout value specified, the function that opens or accesses a message will fail. If you experience frequent timeouts, increase the timeout value.

**Note:** This option is only available for Exchange 5.5.

### Exchange Background Scanning

Indicates whether the information store needs to scan the attachments table to locate attachments that have not yet been scanned, or if a version change has been made.

**Note:** In Exchange 5.5, the option will stop momentarily (0-60 seconds), then restart again. This will not happen in Exchange 2000 or 2003.

**Note:** Background scanning can cause significant performance degradation on the server. It is strongly recommended that you do not enable background scanning on the Exchange server.

## Statistics Tab

Use the Statistics tab to view current statistics for realtime scanning. These summary statistics provide cumulative information about Realtime Monitor activity, including the number of infections found, the number of emails and files scanned, and the infection treatment actions taken.

This tab contains the following fields:

### **List of statistics**

Lists statistical information about realtime scans such as the number of emails scanned, attachments blocked, files of different types scanned, and files infected. It also shows the number of infected files treated with each of the available cure options.

### **Disable Statistics**

Indicates whether to disable the feature tracking realtime statistics.

This tab contains the following unique button:


### **Reset**

Resets the information displayed on the tab to all zeros (0).

## Local Scanning

The Exchange Option supports local scanning and setting changes. The Email Options dialog has two tabs for configuring local email scanning.

### Access the Email Options Dialog

To access the Email Options dialog, click the  icon on the toolbar.

## Options Tab

Use the Options tab to select a subset of messages to scan.

This tab contains the following field:

### **Date/Time**

Lets you select a subset of messages based on the messages' time stamps. The following options are available:

#### **All Messages**

Scans all messages regardless of their time stamps.

#### **Messages dated after:**

Lets you specify a date and time from which to start scanning messages.

#### **Start from last mailbox scanned**

Scans all messages dated since the last time you ran a mail scan.

## Log Tab

Use the Log subtab to specify how to manage log files. You can select to store information about files that are not infected, infected, or not examined.

This tab contains the following fields:

### **Clean Files**

Indicates whether the log should contain information about files that are scanned and not infected.

### **Infected Files**

Indicates whether the log should contain information about files that are found to be infected.

### **Skipped Files**

Indicates whether the log should contain information about files that are excluded from the scan.

### **Show summary dialog box after each scan**


Displays a dialog box with scan results after each scheduled mail scan that shows the number above.

## Scheduled Scanning

The Exchange Option supports scheduled scanning and setting changes. A list of scheduled scan jobs displays in the right pane when you select the Scheduled Scan Jobs category in the left pane.

The Scheduled Scan Job Options dialog has five tabs for configuring scheduled scan jobs.

### Access the Scheduled Scan Job Options Dialog

To access the Scheduled Scan Job Options dialog, click the  icon on the toolbar.

### Description Tab

Use the Description tab to provide a description of the scan job. This description is used to identify the scan job in the Scheduled Scan Jobs list and in the Log Viewer.

This tab contains the following field:

**Enter a description for these settings**

Specifies a description to associate with the scan job.

### Options Tab

Use the Options tab to select a subset of messages to scan.

This tab contains the following field:

**Date/Time**

Lets you select a subset of messages based on the messages' time stamps. The following options are available:

**All Messages**

Scans all messages regardless of their time stamps.

**Messages dated after:**

Lets you specify a date and time from which to start scanning messages.

**Start from last mailbox scanned**

Scans all messages dated since the last time you ran a mail scan.

## Schedule Tab

Use the Schedule tab to specify the date and time for a scan, and to specify the schedule for periodic scan operations.

This tab contains the following fields:

### **Stop this job if it's not done in \_ hours \_ minutes**

Lets you end a scheduled scan job if it is taking too long. Indicate how many hours and minutes to attempt the job before timing out.

### **Date**

Specifies the month, day, and year for the job.

### **Time**

Specifies the time of day for the job, in hours, minutes, and seconds.

### **Repeat Every**

Specifies how often to run a periodic scan job. You can schedule a scan job to run at a regularly scheduled time, specified by months, days, hours, or minutes. You may want to schedule weekly scans for all drives and more frequent scans for drives or directories that have a lot of incoming and outgoing traffic. If you need to rapidly check suspect files, you could schedule a scan that runs every few minutes.

**Note:** The settings for the Date and Time fields determine the first occurrence of the repeat scan.

### **CPU Usage Level**

Specifies the CPU usage level for a scheduled scan job (low, medium, or high usage) on Windows systems. During high production times, you might want a low level of CPU usage for a scan. During low production times, you might want to schedule a higher priority.

## Include Mailboxes Tab

Use the Include Mailboxes tab to choose the databases or mailboxes to include in the scan. It is not necessary to choose the parent database in order to select a child database or mailbox. However, all mailboxes in a selected database are scanned.

This tab contains the following field:

### **List of databases and mailboxes**

Lists the available databases and mailboxes in the left pane. Highlight the appropriate ones, one at a time, and move them to the right pane by clicking the right-facing double arrow.

## Exclude Mailboxes Tab

Use the Exclude Mailboxes tab to choose the databases or mailboxes to exclude from the scan. It is not necessary to choose the parent database in order to select a child database or mailbox.

This tab contains the following field:

### **List of databases and mailboxes**

Lists the available databases and mailboxes in the left pane. Highlight the appropriate ones, one at a time, and move them to the right pane by clicking the right-facing double arrow.

## Scheduled Job Statistics Dialog

The Scheduled Job Statistics dialog displays information about the scheduled scan job that is running. If a scheduled scan job is not currently running, the dialog does not display the statistics. After a scheduled scan is completed, use the Log Viewer to view information about the job.

This dialog displays the following fields:

### **Current Directory**

Indicates the directory or directories being scanned by the current scan job.

### **List of statistics**

Displays summary statistics, including the total number of infections found (reported only, cured, deleted, quarantined, and renamed) and the number of files scanned.

## Detailed Result For Dialog

The Detailed Result For dialog displays detailed information about the infected file selected in the bottom pane of the Scanner window after a scan is run.

This dialog displays the following fields:

**Original Full Path**

Shows the full directory path of where the file was originally located.

**New Full Path**

Shows the full directory path of the where the file has been quarantined, if applicable.

**Infection Name**

Shows the name of the infection found in this file.

**Engine**

Indicates the scanning engine used for the scan that located this file.

**Detection Method**

Indicates the method used to detect this infection, such as signatures or DAT files.

**Infection Type**

Describes the type of infection that was found, such as Virus, Worm, or Trojan.

**Infected Object**

Indicates the type of object in which the infection was found, such as a file or a macro.

**Status**

Shows the current status of the infected file, such as Infected, Cured, or Suspicious.

**Safety Level**

Shows the safety level of the infected file, such as Secure or Reviewer (in the Shell Scanner only).

This dialog displays the following buttons:

**Cure**

Attempts to cure an infected file automatically. Even if the infected file is cured, it is recommended that you delete the infected file and then restore the original file from a backup. If the infected file is from a software package, restore the file from the product installation disks.

**Delete**

Deletes an infected file.

**Rename**

Renames an infected file with an AVB extension. Infected files with the same name are given incremental extensions in the form #.AVB (for example, FILE.0.AVB, FILE.1.AVB, and so on). After a file is renamed with an AVB extension, it is not scanned subsequently.

**Quarantine**

Moves an infected file from its current directory to the Quarantine folder.

**Up**

Changes to display detail information for the previous infected file in the list on the Mail Scanner window.

**Down**

Changes to display detail information for the next infected file in the list on the Mail Scanner window.

## Scan Result Summary Dialog

The Scan Result Summary dialog displays scan data and infection information about the most recent scan job performed.

This dialog displays the following field:

**List of statistics**

Displays summary statistics, including the total number of infections found (reported only, cured, deleted, quarantined, and renamed) and the number of files scanned.

## Logging

The following dialog is available from the Log Viewer window:

- Purge Logs

## Purge Logs Dialog

Use the Purge Logs dialog to indicate whether to have automatic purges of your eTrust Antivirus log files and, if so, how often.

This dialog contains the following fields:

### **Do not delete log files**

Indicates that you want to keep all log files until you decide to manually delete them.

### **Delete all log files that are older than**

Specifies how many days you want the log files to be stored until they are automatically purged.

## Customizable Warning Messages

eTrust Antivirus enables you to modify the text displayed to a user when a virus has been detected. To customize warning messages, you can edit the message strings in the mrtconfig.ini file using a text editor. Refer to the mrtconfig.ini file in the installation directory or the sample file included in this guide for a description of the message strings and options available.

## Sample MRTCONFIG.INI

The following is a sample file for customizing warning messages to be used with your Microsoft Exchange messaging option, if applicable.

-----  
-----

;NOTE: Do not modify this file unless you know what you are doing.

; All messages should be accounted for and none of these message

; strings should be left empty.

;These message strings are used for the AV-ScanReport.txt file

;The length of each string can not exceed 512 bytes.

### **[ReportStrings]**

;Note: Values in <> are variables and should not be altered. However, their order does

; not matter. For instance:

; MsgReport=<FileName> is infected with <VirusName>.

MsgReport=The [<VirusName>] virus was detected in [<FileName>].

MsgCureOK=Original file [<FileName>] was successfully cured.

MsgCureFail=Failed to cure original file [<FileName>].

MsgDelete=Original file [<FileName>] was deleted.

MsgRename=Original file [<FileName>] was renamed to [<NewFileName>].

MsgMove=The infected file [<FileName>] was moved.

MsgBlock=[<FileName>] is being blocked.

MsgEncryptedArc=Encrypted file found in [<FileName>].

;These message strings are only valid for MS Exchange 2k

;The length of each string cannot exceed 128 bytes.

### **[MSExchange2KStrings]**

;The following strings are used for the display name property tags of each attachment.

;This is usually the file name of the attachment. However, the Exchange Option will

;change this tag according to the scan result.

BlockedFile=File is blocked.

VirusDetected=Virus detected.

DefaultFileName=CA-DefaultFileName

EmailBody=Email Body

;The following strings are used for the Application Event Log.

;Do not modify these strings.

**[EventStrings]**

EventStart=Starting %s. Thread ID: %d

EventEnd=Unloading %s. Thread ID: %d

EventReport=The [%s] virus found in [%s] was left alone. The action was to report only.

EventCopyB4Cure=[%s] file with [%s] virus was cure and backup was made.

EventCure=The attachment, [%s], containing the virus, [%s], has been cured.

EventNotCuredRename=The [%s] virus found in [%s] could not be cured. The action was to rename the attachment.

EventNotCuredMove=The [%s] virus found in [%s] could not be cured. The action was to move it.

EventNotCuredNoAction=The [%s] virus found in [%s] could not be cured. There was no action taken.

EventRename=The file, [%s], containing the virus, [%s], was renamed.

EventDelete=The file [%s] containing the virus [%s] was deleted.

EventMove=The file [%s] containing the virus [%s] was moved.

EventBlock=The file [%s] is being blocked.

# Chapter 6: Setting Notes Options

---


This chapter describes the features specific to the Notes Option, and how to guard your system from infections in emails or in your mailbox database.

For more information about managing email options from the administrator console of eTrust Antivirus, see the *eTrust Antivirus Administrator Guide*.

## Realtime Scanning

The Notes Option supports realtime scanning and setting changes through the Realtime Monitor options in the system tray. The Realtime Mail Options dialog has four tabs for managing realtime email scans.

### Access the Realtime Mail Options Dialog

To access the Realtime Mail Options dialog, click the  icon on the toolbar.

Alternately, right-click the Realtime Monitor icon in the system tray and choose Mail Options from the pop-up menu.

## Scan Tab

Use the Scan tab to choose your scanning engine, specify a safety level, and perform file actions.

This tab contains the following fields:

### Incoming and Outgoing Messages

Enables realtime scanning by the email option. If this option is disabled, there is no email protection.

### Scanning Engine

Lets you choose the scanning engine to use, if a choice is available. The scanning engine is the specialized processor that does the work of looking for infections. The installation process automatically selects the appropriate scanning engine for your configuration. Most users do not need to change this option. It is primarily for advanced corporate users at large enterprises. The following engines may be available:

#### InoculateIT

Specifies the base eTrust Antivirus scanning module typically used.

#### Vet

Specifies an alternative scanning module.

### Heuristic Scanner

Includes the Heuristic Scan engine in realtime scanning. The Heuristic Scan engine scans for infections whose signatures have not yet been isolated or documented.

### Specify how thorough the scan should be

You can set the scan safety level to Secure or Reviewer mode. Use the Secure mode as the standard method for scanning files completely.

If you suspect you have an infection that is not being detected by the Secure mode, you can use the Reviewer mode. The Reviewer mode is used to detect a virus that is inactive or deliberately modified, such as in a virus testing laboratory. In addition, Reviewer mode runs significantly slower than Secure mode.

**Note:** In unique circumstances, Reviewer mode can generate a false alarm. Therefore, if you are using this mode as your standard scanning option, use it with the Report Only option.

### File Actions

Indicates how to treat the infection. The following infected file actions are available:

**Report Only**

Reports when an infection is found. If you want to know if there are any infections before you decide what to do with an infected file, choose the Report Only infection treatment. If an infection is found, you can then choose any of the other available treatments.

**Delete File**

Deletes an infected file.

**Rename File**

Renames an infected file with an AVB extension. Infected files with the same name are given incremental extensions in the form #.AVB (for example, FILE.0.AVB, FILE.1.AVB, and so on). After a file is renamed with an AVB extension, it is not scanned subsequently.

**Quarantine File**

Moves an infected file from its current directory to the Quarantine folder.

**Cure File**

Attempts to cure an infected file automatically. Even if the infected file is cured, it is recommended that you delete the infected file and then restore the original file from a backup. If the infected file is from a software package, restore the file from the product installation disks.

This tab contains the following unique button:

**Cure Options**

Opens the Cure Action Options dialog so you can specify how to cure the file. This button is only available if Cure File was chosen as your infection treatment.

## Cure Action Options Dialog

Use the Cure Action Options dialog to specify how to deal with macro viruses and Trojan infections, and what actions to perform before or after a cure is attempted.

This dialog contains the following fields:

### **Copy File**

Copies the file to the Quarantine folder before the cure is attempted.

### **Action to perform if cure fails**

Indicates the actions to perform if a cure fails. The following actions are available:

#### **No action**

Leaves the infected file as is.

#### **Quarantine file**

Moves the infected file into the Quarantine folder.

#### **Rename file**

Renames the infected file with an AVB extension.

### **Cure by Deleting**

Deletes the infected file when a Trojan or Worm infection is found.

### **Macro viruses treatment**

Indicates how to treat macro viruses. The following methods are available:

#### **Remove infected macros**

Removes only infected macros from the file.

#### **Remove all macros**

Removes all macros from the file.

## Selection Tab

Use the Selection tab to choose types of file extensions to include or exclude from a scan and types of compressed files to scan.

This tab contains the following fields:

### **Regular Files**

Indicates what subset of file extensions to scan. Each option has its own list of default extensions. The following subsets are available:

#### **All Extensions**

Scans files with all types of extensions.

#### **Specified Extensions Only**

Scans files with the specified file extensions only.

#### **All Except the Specified Extensions**

Scans files with all types of extensions except those specified.

### **Scan Compressed Files**

Enables you to scan compressed files. Select the Scan Compressed Files check box and then indicate the extensions for the types of compressed files.

This tab contains the following unique buttons:

#### **Edit List**

Depending on your selection for Regular Files, opens either the Specified Extensions Only dialog or the All Except the Specified Extensions dialog to let you add or remove file extensions for scanning.

#### **Options**

Opens the Compressed File Options dialog, where you can specify additional management information for compressed files.

#### **Choose Type**

Opens the Compressed File Type dialog, where you can select the compressed file types to allow in a scan.

#### **Block**

Opens the Block Extension List dialog, where you can specify file extensions to block from the scan.

#### **Exempt**

Opens the Exempt From Blocking dialog, where you can specify particular files to include in the scan even though their extensions are blocked.

## Specified Extensions Only Dialog

Use the Specified Extensions Only dialog to specify file extensions to include in a regular file scan.

This dialog contains the following fields:

### **Enter a new file extension**

Indicates the file extension to add to the list of file extensions.

### **List of File Extensions**

Displays the current file extensions selected. Extensions can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file extension specified in the Enter a new file extension field to the list.

### **Remove**

Removes one or more file extensions from the list. To specify the appropriate extensions, select the check boxes to their left.

## All Except the Specified Extensions Dialog

Use the All Except the Specified Extensions dialog to specify file extensions to exclude from the regular file scan.

This dialog contains the following fields:

### **Enter a new file extension**

Indicates the file extension to add to the list of file extensions.

### **List of File Extensions**

Displays the current file extensions selected. Extensions can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file extension specified in the Enter a new file extension field to the list.

### **Remove**

Removes one or more file extensions from the list. To specify the appropriate extensions, select the check boxes to their left.

## Compressed File Options Dialog

Use the Compressed File Options dialog to set additional options managing compressed files. These can be used to improve scan performance.

This dialog contains the following fields:

### **Apply extension filter to files inside archives**

Scans compressed files based on the list of regular files selected on the Selection subtab.

### **Stop scanning archive when an infected file is found**

Stops scanning the compressed file archive when an infected file is found in it.

### **Apply infection actions to archives**

Applies specified infection treatment options, other than Cure File, to compressed files in the archive.

### **The file's Extension (faster)**

Scans compressed files by recognizing them by extension, which is faster than analyzing them by the contents of the archive.

### **The file's Contents (slower)**

Scans compressed files by analyzing the contents, which is slower than recognizing them by extension.

## Compressed File Type Dialog

Use the Compressed File Type dialog to indicate which compressed file types to include in your scan. The compressed file types that are currently supported for scanning include:

- ARJ
- GZIP
- LHA
- Microsoft cabinet file
- Microsoft compressed file
- MIME
- ZIP or Java archive
- RAR
- UNIX compressed file (.Z)
- TNEF encapsulated eMail files
- TAR
- CA Zip
- BZIP
- self extracting archive

This dialog contains the following fields:

### **File types**

Lets you compile a list of compressed file types that you want the scanner to include. Select and clear the appropriate check boxes.

### **Common file extensions for the selected type**

Displays all applicable extensions for the file type to which you are currently pointing, such as CAB for Microsoft cabinet file.

## Block Extension List Dialog

Use the Block Extension List dialog to specify file extensions to block. When a file extension is blocked, any file with that extension is not scanned and all access to the file is denied.

This dialog contains the following fields:

### **Enter a new file extension**

Indicates the file extension to add to the list of file extensions.

### **List of blocked extensions**

Displays the current file extensions selected. Extensions can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file extension specified in the Enter a new file extension field to the list.

### **Remove**

Removes one or more file extensions from the list. To specify the appropriate extensions, select the check boxes to their left.

## Exempt from Blocking Dialog

Use the Exempt from Blocking dialog to include one or more files in realtime scanning even though the associated file extension is included in the pre-scan block list.

This dialog contains the following fields:

### **Enter an email attachment's file name**

Indicates the file name of the email attachment to add to the list of exempt files. These files are scanned and then delivered even if their extensions are specified in the blocked list.

### **List of Exempt Files**

Displays the current files selected for exemption. Files can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file specified in the field to the list.

### **Remove**

Removes the selected file from the list.

## Notification Tab

Use the Notification tab to specify notification options. eTrust Antivirus sends out the types of notifications you specify using the Lotus Notes Domino Option mail system whenever an infection is detected in the messaging system.

This tab contains the following fields:

### **Notify Mailbox Owner**

Indicates whether to notify the person who received the mail that an infection was attached. This check box is always selected and cannot be modified.

### **Notify Message Sender**

Indicates whether to notify the user who sent the infected mail or created the database containing the infection. By using this option, you can track the infected file to its origin, and notify the owner of the mailbox that originally mailed the infected file.

### **Notify Mail System Administrators**

Indicates whether to notify specified system administrators that network security might have been violated. The administrators can then take whatever actions are needed to secure the network.

### **Insert Note as Attachment**

Lets you add another note to the email message as an attachment. The note provides information about the infected file, what action was taken, and whether it was cured.

### **Send scan results to generate reports**

Indicates whether the scan results should be forwarded, allowing them to be used to generate reports.

### **Return to Address**

Indicates where to reroute a notification if it is undeliverable to the original address.

### **Default Subject**

Specifies the subject for the notification.

This tab contains the following unique button:

### **Administrators**

Opens the Notify Administrators dialog so you can enter a list of administrators to notify with security issues.

## Notify Administrators Dialog

Use the Notify Administrators dialog to specify administrators to contact when there is a mail-related security concern.

This dialog contains the following fields:

### **Enter an email address**

Specifies the email address at which to contact the administrator.

### **List of administrators**

Lists the administrators that are notified when there is a security concern.

This dialog contains the following unique buttons:

### **Add**

Adds the email address in the Enter an email address field to the List of administrators box.

### **Remove**

Removes the highlighted email address from the List of administrators box.

## Statistics Tab

Use the Statistics tab to view current statistics for realtime scanning. These summary statistics provide cumulative information about Realtime Monitor activity, including the number of infections found, the number of emails and files scanned, and the infection treatment actions taken.

This tab contains the following fields:

### **List of statistics**

Lists statistical information about realtime scans such as the number of emails scanned, attachments blocked, files of different types scanned, and files infected. It also shows the number of infected files treated with each of the available cure options.

### **Disable Statistics**

Indicates whether to disable the feature tracking realtime statistics.

This tab contains the following unique button:

### **Reset**

Resets the information displayed on the tab to all zeros (0).

## Local Scanning

The Notes Option supports local scanning and setting changes. The Email Options dialog has five tabs for configuring local email scanning.

### Access the Email Options Dialog

To access the Email Options dialog, click the  icon on the toolbar.

## Scan Tab

Use the Scan tab to enable the mail option, choose your scanning engine, specify a safety level, and perform desired file actions.

This tab contains the following fields:

### **Specify how thorough the scan should be**

You can set the scan safety level to Secure or Reviewer mode. Use the Secure mode as the standard method for scanning files completely.

If you suspect you have an infection that is not being detected by the Secure mode, you can use the Reviewer mode. The Reviewer mode is used to detect a virus that is inactive or deliberately modified, such as in a virus testing laboratory. In addition, Reviewer mode runs significantly slower than Secure mode.

**Note:** In unique circumstances, Reviewer mode can generate a false alarm. Therefore, if you are using this mode as your standard scanning option, use it with the Report Only option.

### **Scanning Engine**

Lets you choose the scanning engine to use, if a choice is available. The scanning engine is the specialized processor that does the work of looking for infections. The installation process automatically selects the appropriate scanning engine for your configuration. Most users do not need to change this option. It is primarily for advanced corporate users at large enterprises. The following engines may be available:

#### **InoculateIT**

Specifies the base eTrust Antivirus scanning module typically used.

#### **Vet**

Specifies an alternative scanning module.

### **Heuristic Scanner**

Includes the Heuristic Scan engine in realtime scanning. The Heuristic Scan engine scans for infections whose signatures have not yet been isolated or documented.

### **File Actions**

Indicates how to treat the infection. The following infected file actions are available:

#### **Report Only**

Reports when an infection is found. If you want to know if there are any infections before you decide what to do with an infected file, choose the Report Only infection treatment. If an infection is found, you can then choose any of the other available treatments.

#### **Delete File**

Deletes an infected file.

**Rename File**

Renames an infected file with an AVB extension. Infected files with the same name are given incremental extensions in the form #.AVB (for example, FILE.0.AVB, FILE.1.AVB, and so on). After a file is renamed with an AVB extension, it is not scanned subsequently.

**Quarantine File**

Moves an infected file from its current directory to the Quarantine folder.

**Cure File**

Attempts to cure an infected file automatically. Even if the infected file is cured, it is recommended that you delete the infected file and then restore the original file from a backup. If the infected file is from a software package, restore the file from the product installation disks.

This tab contains the following unique button:

**File Options**

Opens the Cure Action Options dialog so you can specify how to cure the file. This button is only available if Cure File was chosen as your infection treatment.

## Cure Action Options Dialog

Use the Cure Action Options dialog to specify how to deal with macro viruses and Trojan infections, and what actions to perform before or after a cure is attempted.

This dialog contains the following fields:

### **Copy File**

Copies the file to the Quarantine folder before the cure is attempted.

### **Action to perform if cure fails**

Indicates the actions to perform if a cure fails. The following actions are available:

#### **No action**

Leaves the infected file as is.

#### **Quarantine file**

Moves the infected file into the Quarantine folder.

#### **Rename file**

Renames the infected file with an AVB extension.

### **Cure by Deleting**

Deletes the infected file when a Trojan or Worm infection is found.

### **Macro viruses treatment**

Indicates how to treat macro viruses. The following methods are available:

#### **Remove infected macros**

Removes only infected macros from the file.

#### **Remove all macros**

Removes all macros from the file.

## Selection Tab

Use the Selection tab to choose types of file extensions to include or exclude from a scan, and types of compressed files to scan.

This tab contains the following fields:

### **Objects to Scan**

Indicates whether to scan files. Files is selected by default. The types of files that are scanned are determined by the extensions you specify to include or exclude using the Regular Files and Scan Compressed Files options.

### **Regular Files**

Indicates what subset of file extensions to scan. Each option has its own list of default extensions. The following subsets are available:

#### **All Extensions**

Scans files with all types of extensions.

#### **Specified Extensions Only**

Scans files with the specified file extensions only.

#### **All Except the Specified Extensions**

Scans files with all types of extensions except those specified.

### **Scan Compressed Files**

Enables you to scan compressed files. Select the Scan Compressed Files check box and then indicate the extensions for the types of compressed files.

This tab contains the following unique buttons:

### **Edit List**

Depending on your selection for Regular Files, opens either the Specified Extensions Only dialog or the All Except the Specified Extensions dialog to let you add or remove file extensions for scanning.

### **Options**

Opens the Compressed File Options dialog, where you can specify additional management information for compressed files.

### **Choose Type**

Opens the Compressed File Type dialog, where you can select the compressed file types to allow in a scan.

## Specified Extensions Only Dialog

Use the Specified Extensions Only dialog to specify file extensions to include in a regular file scan.

This dialog contains the following fields:

### **Enter a new file extension**

Indicates the file extension to add to the list of file extensions.

### **List of File Extensions**

Displays the current file extensions selected. Extensions can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file extension specified in the Enter a new file extension field to the list.

### **Remove**

Removes one or more file extensions from the list. To specify the appropriate extensions, select the check boxes to their left.

## All Except the Specified Extensions Dialog

Use the All Except the Specified Extensions dialog to specify file extensions to exclude from the regular file scan.

This dialog contains the following fields:

### **Enter a new file extension**

Indicates the file extension to add to the list of file extensions.

### **List of File Extensions**

Displays the current file extensions selected. Extensions can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file extension specified in the Enter a new file extension field to the list.

### **Remove**

Removes one or more file extensions from the list. To specify the appropriate extensions, select the check boxes to their left.

## Compressed File Options Dialog

Use the Compressed File Options dialog to set additional options managing compressed files. These can be used to improve scan performance.

This dialog contains the following fields:

### **Apply extension filter to files inside archives**

Scans compressed files based on the list of regular files selected on the Selection subtab.

### **Stop scanning archive when an infected file is found**

Stops scanning the compressed file archive when an infected file is found in it.

### **Apply infection actions to archives**

Applies specified infection treatment options, other than Cure File, to compressed files in the archive.

### **The file's Extension (faster)**

Scans compressed files by recognizing them by extension, which is faster than analyzing them by the contents of the archive.

### **The file's Contents (slower)**

Scans compressed files by analyzing the contents, which is slower than recognizing them by extension.

## Compressed File Type Dialog

Use the Compressed File Type dialog to indicate which compressed file types to include in your scan. The compressed file types that are currently supported for scanning include:

- ARJ
- GZIP
- LHA
- Microsoft cabinet file
- Microsoft compressed file
- MIME
- ZIP or Java archive
- RAR
- UNIX compressed file (.Z)
- TNEF encapsulated eMail files
- TAR
- CA Zip
- BZIP
- self extracting archive

This dialog contains the following fields:

### **File types**

Lets you compile a list of compressed file types that you want the scanner to include. Select and clear the appropriate check boxes.

### **Common file extensions for the selected type**

Displays all applicable extensions for the file type to which you are currently pointing, such as CAB for Microsoft cabinet file.

## Options Tab

Use the Options tab to select a subset of messages to scan.

This tab contains the following field:

### **Date/Time**

Lets you select a subset of messages based on the messages' time stamps. The following options are available:

#### **All Messages**

Scans all messages regardless of their time stamps.

#### **Messages dated after:**

Lets you specify a date and time from which to start scanning messages.

#### **Start from last mailbox scanned**

Scans all messages dated since the last time you ran a mail scan.

## Log Tab

Use the Log subtab to specify how to manage log files. You can select to store information about files that are not infected, infected, or not examined.

This tab contains the following fields:

### **Clean Files**

Indicates whether the log should contain information about files that are scanned and not infected.

### **Infected Files**

Indicates whether the log should contain information about files that are found to be infected.

### **Skipped Files**

Indicates whether the log should contain information about files that are excluded from the scan.

### **Show summary dialog box after each scan**

Displays a dialog box with scan results after each scheduled mail scan that shows the number above.

## Notification Tab

Use the Notification tab to specify notification options. eTrust Antivirus sends out the types of notifications you specify using the Lotus Notes Domino Option mail system whenever an infection is detected in the messaging system.

This tab contains the following fields:

### **Notify Mailbox Owner**

Indicates whether to notify the person who received the mail that an infection was attached. This check box is always selected and cannot be modified.

### **Notify Message Sender**

Indicates whether to notify the user who sent the infected mail or created the database containing the infection. By using this option, you can track the infected file to its origin, and notify the owner of the mailbox that originally mailed the infected file.

### **Notify Mail System Administrators**

Indicates whether to notify specified system administrators that network security might have been violated. The administrators can then take whatever actions are needed to secure the network.

### **Insert Note as Attachment**

Lets you add another note to the email message as an attachment. The note provides information about the infected file, what action was taken, and whether it was cured.

### **Send scan results to generate reports**

Indicates whether the scan results should be forwarded, allowing them to be used to generate reports.

### **Return to Address**

Indicates where to reroute a notification if it is undeliverable to the original address.

### **Default Subject**

Specifies the subject for the notification.

This tab contains the following unique button:

### **Administrators**

Opens the Notify Administrators dialog so you can enter a list of administrators to notify with security issues.

## Notify Administrators Dialog

Use the Notify Administrators dialog to specify administrators to contact when there is a mail-related security concern.

This dialog contains the following fields:

### **Enter an email address**

Specifies the email address at which to contact the administrator.

### **List of administrators**

Lists the administrators that are notified when there is a security concern.

This dialog contains the following unique buttons:

### **Add**

Adds the email address in the Enter an email address field to the List of administrators box.

### **Remove**


Removes the highlighted email address from the List of administrators box.

## Scheduled Scanning

The Notes Option supports scheduled scanning and setting changes. A list of scheduled scan jobs displays in the right pane when you select the Scheduled Scan Jobs category in the left pane.

The Scheduled Scan Job Options dialog has eight tabs for configuring scheduled scan jobs.

## Access the Scheduled Scan Job Options Dialog

To access the Scheduled Scan Job Options dialog, click the  icon on the toolbar.

## Description Tab

Use the Description tab to provide a description of the scan job. This description is used to identify the scan job in the Scheduled Scan Jobs list and in the Log Viewer.

This tab contains the following field:

**Enter a description for these settings**

Specifies a description to associate with the scan job.

## Scan Tab

Use the Scan tab to enable the mail option, choose your scanning engine, specify a safety level, and perform desired file actions.

This tab contains the following fields:

### **Specify how thorough the scan should be**

You can set the scan safety level to Secure or Reviewer mode. Use the Secure mode as the standard method for scanning files completely.

If you suspect you have an infection that is not being detected by the Secure mode, you can use the Reviewer mode. The Reviewer mode is used to detect a virus that is inactive or deliberately modified, such as in a virus testing laboratory. In addition, Reviewer mode runs significantly slower than Secure mode.

**Note:** In unique circumstances, Reviewer mode can generate a false alarm. Therefore, if you are using this mode as your standard scanning option, use it with the Report Only option.

### **Scanning Engine**

Lets you choose the scanning engine to use, if a choice is available. The scanning engine is the specialized processor that does the work of looking for infections. The installation process automatically selects the appropriate scanning engine for your configuration. Most users do not need to change this option. It is primarily for advanced corporate users at large enterprises. The following engines may be available:

#### **InoculateIT**

Specifies the base eTrust Antivirus scanning module typically used.

#### **Vet**

Specifies an alternative scanning module.

### **Heuristic Scanner**

Includes the Heuristic Scan engine in realtime scanning. The Heuristic Scan engine scans for infections whose signatures have not yet been isolated or documented.

### **File Actions**

Indicates how to treat the infection. The following infected file actions are available:

#### **Report Only**

Reports when an infection is found. If you want to know if there are any infections before you decide what to do with an infected file, choose the Report Only infection treatment. If an infection is found, you can then choose any of the other available treatments.

**Delete File**

Deletes an infected file.

**Rename File**

Renames an infected file with an AVB extension. Infected files with the same name are given incremental extensions in the form #.AVB (for example, FILE.0.AVB, FILE.1.AVB, and so on). After a file is renamed with an AVB extension, it is not scanned subsequently.

**Quarantine File**

Moves an infected file from its current directory to the Quarantine folder.

**Cure File**

Attempts to cure an infected file automatically. Even if the infected file is cured, it is recommended that you delete the infected file and then restore the original file from a backup. If the infected file is from a software package, restore the file from the product installation disks.

This tab contains the following unique button:

**File Options**

Opens the Cure Action Options dialog so you can specify how to cure the file. This button is only available if Cure File was chosen as your infection treatment.

## Cure Action Options Dialog

Use the Cure Action Options dialog to specify how to deal with macro viruses and Trojan infections, and what actions to perform before or after a cure is attempted.

This dialog contains the following fields:

### **Copy File**

Copies the file to the Quarantine folder before the cure is attempted.

### **Action to perform if cure fails**

Indicates the actions to perform if a cure fails. The following actions are available:

#### **No action**

Leaves the infected file as is.

#### **Quarantine file**

Moves the infected file into the Quarantine folder.

#### **Rename file**

Renames the infected file with an AVB extension.

### **Cure by Deleting**

Deletes the infected file when a Trojan or Worm infection is found.

### **Macro viruses treatment**

Indicates how to treat macro viruses. The following methods are available:

#### **Remove infected macros**

Removes only infected macros from the file.

#### **Remove all macros**

Removes all macros from the file.

## Selection Tab

Use the Selection tab to choose types of file extensions to include or exclude from a scan, and types of compressed files to scan.

This tab contains the following fields:

### **Objects to Scan**

Indicates whether to scan files. Files is selected by default. The types of files that are scanned are determined by the extensions you specify to include or exclude using the Regular Files and Scan Compressed Files options.

### **Regular Files**

Indicates what subset of file extensions to scan. Each option has its own list of default extensions. The following subsets are available:

#### **All Extensions**

Scans files with all types of extensions.

#### **Specified Extensions Only**

Scans files with the specified file extensions only.

#### **All Except the Specified Extensions**

Scans files with all types of extensions except those specified.

### **Scan Compressed Files**

Enables you to scan compressed files. Select the Scan Compressed Files check box and then indicate the extensions for the types of compressed files.

This tab contains the following unique buttons:

### **Edit List**

Depending on your selection for Regular Files, opens either the Specified Extensions Only dialog or the All Except the Specified Extensions dialog to let you add or remove file extensions for scanning.

### **Options**

Opens the Compressed File Options dialog, where you can specify additional management information for compressed files.

### **Choose Type**

Opens the Compressed File Type dialog, where you can select the compressed file types to allow in a scan.

## Specified Extensions Only Dialog

Use the Specified Extensions Only dialog to specify file extensions to include in a regular file scan.

This dialog contains the following fields:

### **Enter a new file extension**

Indicates the file extension to add to the list of file extensions.

### **List of File Extensions**

Displays the current file extensions selected. Extensions can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file extension specified in the Enter a new file extension field to the list.

### **Remove**

Removes one or more file extensions from the list. To specify the appropriate extensions, select the check boxes to their left.

## All Except the Specified Extensions Dialog

Use the All Except the Specified Extensions dialog to specify file extensions to exclude from the regular file scan.

This dialog contains the following fields:

### **Enter a new file extension**

Indicates the file extension to add to the list of file extensions.

### **List of File Extensions**

Displays the current file extensions selected. Extensions can be added or removed.

This dialog contains the following unique buttons:

### **Add**

Adds the file extension specified in the Enter a new file extension field to the list.

### **Remove**

Removes one or more file extensions from the list. To specify the appropriate extensions, select the check boxes to their left.

## Compressed File Options Dialog

Use the Compressed File Options dialog to set additional options managing compressed files. These can be used to improve scan performance.

This dialog contains the following fields:

### **Apply extension filter to files inside archives**

Scans compressed files based on the list of regular files selected on the Selection subtab.

### **Stop scanning archive when an infected file is found**

Stops scanning the compressed file archive when an infected file is found in it.

### **Apply infection actions to archives**

Applies specified infection treatment options, other than Cure File, to compressed files in the archive.

### **The file's Extension (faster)**

Scans compressed files by recognizing them by extension, which is faster than analyzing them by the contents of the archive.

### **The file's Contents (slower)**

Scans compressed files by analyzing the contents, which is slower than recognizing them by extension.

## Compressed File Type Dialog

Use the Compressed File Type dialog to indicate which compressed file types to include in your scan. The compressed file types that are currently supported for scanning include:

- ARJ
- GZIP
- LHA
- Microsoft cabinet file
- Microsoft compressed file
- MIME
- ZIP or Java archive
- RAR
- UNIX compressed file (.Z)
- TNEF encapsulated eMail files
- TAR
- CA Zip
- BZIP
- self extracting archive

This dialog contains the following fields:

### **File types**

Lets you compile a list of compressed file types that you want the scanner to include. Select and clear the appropriate check boxes.

### **Common file extensions for the selected type**

Displays all applicable extensions for the file type to which you are currently pointing, such as CAB for Microsoft cabinet file.

## Options Tab

Use the Options tab to select a subset of messages to scan.

This tab contains the following field:

### **Date/Time**

Lets you select a subset of messages based on the messages' time stamps. The following options are available:

#### **All Messages**

Scans all messages regardless of their time stamps.

#### **Messages dated after:**

Lets you specify a date and time from which to start scanning messages.

#### **Start from last mailbox scanned**

Scans all messages dated since the last time you ran a mail scan.

## Schedule Tab

Use the Schedule tab to specify the date and time for a scan, and to specify the schedule for periodic scan operations.

This tab contains the following fields:

### **Stop this job if it's not done in \_ hours \_ minutes**

Lets you end a scheduled scan job if it is taking too long. Indicate how many hours and minutes to attempt the job before timing out.

### **Date**

Specifies the month, day, and year for the job.

### **Time**

Specifies the time of day for the job, in hours, minutes, and seconds.

### **Repeat Every**

Specifies how often to run a periodic scan job. You can schedule a scan job to run at a regularly scheduled time, specified by months, days, hours, or minutes. You may want to schedule weekly scans for all drives and more frequent scans for drives or directories that have a lot of incoming and outgoing traffic. If you need to rapidly check suspect files, you could schedule a scan that runs every few minutes.

**Note:** The settings for the Date and Time fields determine the first occurrence of the repeat scan.

### **CPU Usage Level**

Specifies the CPU usage level for a scheduled scan job (low, medium, or high usage) on Windows systems. During high production times, you might want a low level of CPU usage for a scan. During low production times, you might want to schedule a higher priority.

## Include Directories Tab

Use the Include Directories tab to add folders or database files to a scheduled scan job.

This tab contains the following fields:

**Enter a full directory path or mail database**

Specifies the directory or database to add to the list.

**List of directories and databases**

Lists the directories and databases selected.

This tab contains the following unique buttons:

**Browse Directory**

Opens a tree browser so you can select a directory.

**Browse Database**

Opens a Windows browser with the database file extension (.nsf) selected.

**Add**

Adds the directory or database file in the Enter a full directory path or mail database field to the List of directories and databases box.

**Remove**

Removes the highlighted directory or database file from the List of directories and databases box.

## Exclude Directories Tab

Use the Exclude Directories tab to exclude folders or database files from a scheduled scan job.

This tab contains the following fields:

**Enter a full directory path or mail database**

Specifies the directory or database to add to the list.

**List of directories and databases**

Lists the directories and databases selected.

This tab contains the following unique buttons:

**Browse Directory**

Opens a tree browser so you can select a directory.

**Browse Database**

Opens a Windows browser with the database file extension (.nsf) selected.

**Add**

Adds the directory or database file in the Enter a full directory path or mail database field to the List of directories and databases box.

**Remove**

Removes the highlighted directory or database file from the List of directories and databases box.

## Notification Tab

Use the Notification tab to specify notification options. eTrust Antivirus sends out the types of notifications you specify using the Lotus Notes Domino Option mail system whenever an infection is detected in the messaging system.

This tab contains the following fields:

### **Notify Mailbox Owner**

Indicates whether to notify the person who received the mail that an infection was attached. This check box is always selected and cannot be modified.

### **Notify Message Sender**

Indicates whether to notify the user who sent the infected mail or created the database containing the infection. By using this option, you can track the infected file to its origin, and notify the owner of the mailbox that originally mailed the infected file.

### **Notify Mail System Administrators**

Indicates whether to notify specified system administrators that network security might have been violated. The administrators can then take whatever actions are needed to secure the network.

### **Insert Note as Attachment**

Lets you add another note to the email message as an attachment. The note provides information about the infected file, what action was taken, and whether it was cured.

### **Send scan results to generate reports**

Indicates whether the scan results should be forwarded, allowing them to be used to generate reports.

### **Return to Address**

Indicates where to reroute a notification if it is undeliverable to the original address.

### **Default Subject**

Specifies the subject for the notification.

This tab contains the following unique button:

### **Administrators**

Opens the Notify Administrators dialog so you can enter a list of administrators to notify with security issues.

## Notify Administrators Dialog

Use the Notify Administrators dialog to specify administrators to contact when there is a mail-related security concern.

This dialog contains the following fields:

### **Enter an email address**

Specifies the email address at which to contact the administrator.

### **List of administrators**

Lists the administrators that are notified when there is a security concern.

This dialog contains the following unique buttons:

### **Add**

Adds the email address in the Enter an email address field to the List of administrators box.

### **Remove**

Removes the highlighted email address from the List of administrators box.

## Scheduled Job Statistics Dialog

The Scheduled Job Statistics dialog displays information about the scheduled scan job that is running. If a scheduled scan job is not currently running, the dialog does not display the statistics. After a scheduled scan is completed, use the Log Viewer to view information about the job.

This dialog displays the following fields:

### **Current Directory**

Indicates the directory or directories being scanned by the current scan job.

### **List of statistics**

Displays summary statistics, including the total number of infections found (reported only, cured, deleted, quarantined, and renamed) and the number of files scanned.

## Detailed Result For Dialog

The Detailed Result For dialog displays detailed information about the infected file selected in the bottom pane of the Scanner window after a scan is run.

This dialog displays the following fields:

**Original Full Path**

Shows the full directory path of where the file was originally located.

**New Full Path**

Shows the full directory path of the where the file has been quarantined, if applicable.

**Infection Name**

Shows the name of the infection found in this file.

**Engine**

Indicates the scanning engine used for the scan that located this file.

**Detection Method**

Indicates the method used to detect this infection, such as signatures or DAT files.

**Infection Type**

Describes the type of infection that was found, such as Virus, Worm, or Trojan.

**Infected Object**

Indicates the type of object in which the infection was found, such as a file or a macro.

**Status**

Shows the current status of the infected file, such as Infected, Cured, or Suspicious.

**Safety Level**

Shows the safety level of the infected file, such as Secure or Reviewer (in the Shell Scanner only).

This dialog displays the following buttons:

**Cure**

Attempts to cure an infected file automatically. Even if the infected file is cured, it is recommended that you delete the infected file and then restore the original file from a backup. If the infected file is from a software package, restore the file from the product installation disks.

**Delete**

Deletes an infected file.

**Rename**

Renames an infected file with an AVB extension. Infected files with the same name are given incremental extensions in the form #.AVB (for example, FILE.0.AVB, FILE.1.AVB, and so on). After a file is renamed with an AVB extension, it is not scanned subsequently.

**Quarantine**

Moves an infected file from its current directory to the Quarantine folder.

**Up**

Changes to display detail information for the previous infected file in the list on the Mail Scanner window.

**Down**

Changes to display detail information for the next infected file in the list on the Mail Scanner window.

## Scan Result Summary Dialog


The Scan Result Summary dialog displays scan data and infection information about the most recent scan job performed.

This dialog displays the following field:

**List of statistics**

Displays summary statistics, including the total number of infections found (reported only, cured, deleted, quarantined, and renamed) and the number of files scanned.

## Mail Scanner Folders

The following dialog is available by clicking the  icon on the toolbar:


- Add Folder

Alternately, you can right-click the Domino Server in the left pane of the Mail Scanner window and choose Add Favorite Folder from the pop-up menu.

---

## Add Folder Dialog

Use the Add Folder dialog to add a favorites folder for scanning mail. This enables you to scan data folders other than \Lotus\Domino\Data (Domino Data Folder) and [Program Files]\Lotus\Notes\Data (Notes Data Folder).

**Note:** If you want to remove a folder later, highlight it and click the  icon on the toolbar.

This dialog contains the following fields:

### Folder Description

Indicates what you want the folder to be named on the Mail Scanner view.

### Selected Folder

Indicates the physical path to associate with this description. This folder should contain the mail databases you want to include.

This dialog contains the following unique buttons:

### Browse

Lets you browse to select a folder.

## Logging

The following dialog is available from the Log Viewer window:

- Purge Logs

## Purge Logs Dialog

Use the Purge Logs dialog to indicate whether to have automatic purges of your eTrust Antivirus log files and, if so, how often.

This dialog contains the following fields:

### Do not delete log files

Indicates that you want to keep all log files until you decide to manually delete them.

### Delete all log files that are older than

Specifies how many days you want the log files to be stored until they are automatically purged.

## Customizable Warning Messages

eTrust Antivirus enables you to modify the text displayed to a user when a virus has been detected. To customize warning messages, you can edit the message strings in the `virushdr.txt` file using a text editor. Refer to the `virushdr.txt` file in the installation directory for a description of the message strings and options available. You can also customize the subject of warning messages by editing the text box for Default Subject or the value of `SUBJECT_FOR_INFECTED` in `NotesStr.ini`. Finally, you can customize the return address of warning messages by editing the text box for Return to address or the value of `RETURN_ADDRESS` in the `NotesStr.ini` file.

## Sample NOTESSTR.INI

The following is a sample file for customizing warning messages to be used with your Lotus Notes Domino messaging option, if applicable.

```
[CustomMessage]
SUBJECT_FOR_INFECTIION_RT=Warning (Realtime Scanner): Infected/Block attachment(s)
was detected!
SUBJECT_FOR_INFECTIION_SS=Warning (Schedule Scanner): Infected attachment(s) was
detected!
SUBJECT_FOR_INFECTIION_LS=Warning (Local Scanner): Infected attachment(s) was
detected!
RETURN_ADDRESS=eTrust Antivirus Option For Lotus Notes Domino<Your Return Address
Here>
```

```
[NotesString]
```

```
0 = Undefined
1 = InRouter
2 = Initializing...
3 = Idle...
4 = Routing...
5 = Terminating...
6 = InRouter: Initializing...
7 = InRouter: Initialization complete.
8 = InRouter: Initialization error.
9 = InRouter: Routing complete.
10 = InRouter: Terminating...
11 = InRouter: Termination complete.
12 = InRouter: Thread %d - Stats [Total: %d] [Routed: %d] [Failed: %d]
[Attachments: %d]
```

```
13 = Not Infected
14 = Infected
15 = Unknown infection
16 = Cured
17 = Copied and cured
18 = Cure failed, file restored.
19 = Renamed
20 = Cure failed, file renamed.
21 = Quarantined
22 = Cure failed, file quarantined.
23 = Deleted
24 = Skipped
25 = Pre-copy failed; cure skipped.
26 = Trojan/Worm File Deleted
27 = Virus has damaged the file. Can not fix it.
28 = No cure for this infection
29 = File was cured by system cure and the machine needs to reboot.
```

30 = File was cured by deleting the file generated by virus.

31 = None  
32 = Virus  
33 = Trojan  
34 = Joke  
35 = Worm  
36 = Unknown

37 = None  
38 = Signature  
39 = Heuristics  
40 = Polysearch  
41 = Incremental

42 = InoculateIT  
43 = Vet

44 = Blocked by extension

45 = %s in Database <%s>  
46 = %s%s in Database <%s>

100 = "%s detected infected/blocked attachment(s) in an e-mail from [%s] to [%s] with subject [%s]. Attachment(s): [%s] Status: %s"  
101 = "Warning: \n\nThe e-mail from [%s] to [%s] with subject [%s] may contain virus. We recommend you to use Local Scanner to scan that message. "  
102 = "Warning: \n\nBecause the e-mail from [%s] to [%s] with subject [%s] is encrypted, %s is NOT able to scan it. "  
103 = "%s detected infected/blocked attachment(s) in an e-mail from [%s] to [%s] with subject [%s]. Infected attachment(s): [%s] "  
104 = "Warning from %s! "  
105 = "Warning: The e-mail from [%s] to [%s] with subject [%s] may contain virus. We recommend you to use InoculateIT Local Scanner to scan that message. "  
106 = "Warning: %s detected infected/blocked attachment(s)!"

107 = "Report Only"  
108 = "File Deleted"  
109 = "File Cured"  
110 = "File Cannot be Cured"  
111 = "File Purged"  
112 = "File Renamed"  
113 = "File Quarantined"  
114 = "File Quarantined and Renamed"  
115 = "File Cannot be Cured and Renamed"

116 = "Warning: Because the e-mail from [%s] to [%s] with subject [%s] is encrypted, InoculateIT Lotus Notes Option is NOT able to scan it. "

117 = "%s"  
118 = "Unknown Infection"  
119 = "File Skipped"  
120 = "Pre-copy Failed, Cure Skipped"  
121 = "Trojan/Worm File Deleted"  
122 = "File Cannot be Cured"  
123 = "File was cured by system cure and the machine needs to reboot."  
124 = "File was cured by deleting the file generated by virus."  
125 = "No cure for this infection"  
126 = "File Blocked"

127 = "File: %s"  
128 = "Status: %s"  
129 = "Infection: %s"  
130 = "Type: %s"  
131 = "Method: %s"  
132 = "Engine: %s"  
133 = "Infected Object: %s"  
134 = "%s blocked <%s>!"  
135 = "The beta version of this product will not run because it has expired."

200 = "Starting eTrust Lotus Notes Option realtime scanner."  
201 = "Copyright (c) 2005, Computer Associates International, All Rights Reserved."  
202 = "Stopping eTrust Lotus Notes Option realtime scanner."  
203 = "Found: (%d) new mail(s) in mail(%d).box."  
204 = "Scanning <%s>"  
205 = "Starting eTrust Lotus Notes Option Local Scanner."  
206 = "Starting eTrust Lotus Notes Option Schedule Scanner."  
207 = "Starting eTrust Lotus Notes Option Command Line Scanner."  
208 = "The scan job is done."  
209 = "Usage: InocNote /ls=InocNote.ini (or your own ini file)"  
210 = "The INI file for the scanner can not be found."  
211 = "Failed to open <%s>. Error : %s"



# Index

---

## A

- accessing mail options
  - for local scans • 35
  - for realtime scans • 21
  - for scheduled scans • 37
- add folder dialog • 83
- all except the specified extensions dialog • 26
- antivirus newsletter • 8

## B

- backup
  - system • 8
- block extension list dialog • 53
- block file list dialog • 29

## C

- compressed file options dialog • 27
- compressed file type dialog • 28
- cure action options dialog • 24

## D

- description tab • 37
- detailed result for dialog • 40
- downloading signature files • 8

## E

- email options dialog • 35
- exchange option
  - features • 9
  - installing • 11
  - settings • 21
- exclude directories tab • 78
- exclude mailboxes tab • 39
- exempt from blocking dialog • 30

## F

- features (messaging) • 10

## G

- groupware options • 8

## I

- include directories tab • 77

- include mailboxes tab • 38
- infected file analysis • 40
- installing • 12, 13

## L

- local scanning • 15
- log tab • 36
- log viewer • 19
- logging • 41
- Lotus Notes Option • 10

## M

- mail scanner • 16
- mail scanner folders • 82
- messaging/groupware systems • 7
- Microsoft Exchange option • 9
- misc tab • 34
- move folder • 19
- MRTCONFIG.INI • 43

## N

- notes option
  - features • 10
  - installing • 13
  - settings for • 45
- notification tab • 31, 54
- notify administrators dialog • 32

## O

- options tab • 33, 36

## P

- protecting your network • 8
- purge logs dialog • 42

## Q

- quarantine folder • 19

## R

- realtime mail options dialog • 21
- realtime scanning • 15

## S

- scan tab • 22, 57

---

- schedule tab • 38
- scheduled job statistics dialog • 39
- scheduled scan job options dialog • 37
- scheduled scanning • 16
- scheduled scans
  - job statistics • 39
- selection tab • 25, 60
- show last scan summary • 19
- specified extensions only dialog • 26
- statistics tab • 35

## T

- technical support • 8
- testing the installation • 12, 14