
IMail Anti-Virus

Setup Guide

Software Version V1.10

Ipswitch, Inc.

Ipswitch, Inc.
10 Maguire Road
Suite 220
Lexington, MA 02421-3110

Phone: 781-676-5700
Fax: 781-676-5710
Web: <http://www.ipswitch.com>

Copyrights

The information in this document is subject to change without notice and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc. assumes no liability for damages resulting from the use of the information contained in this document. The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of that license.

Copyright © 1995-2003 by Ipswitch, Inc. All rights reserved. IMail, the IMail logo, WhatsUp, the WhatsUp logo, WS_FTP, the WS_FTP logos, Ipswitch Instant Messaging (IM), Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Other products or company names are or may be trademarks or registered trademarks and are the property of their respective companies.

Symantec, LiveUpdate, Symantec AntiVirus Scan Engine 4.0, CarrierScan Server, and Bloodhound are registered trademarks of Symantec Corporation.

No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transferred without the expressed prior written consent of Ipswitch, Inc.

Printing History

November, 2001	First edition
September, 2003	Second edition

Contents

Setting Up IMail Anti-Virus	1
What is IMail Anti-Virus?	1
Frequently Asked Questions	2
Overview of Setup Tasks	3
Installation Process	4
Minimum System Requirements	4
Before You Install	4
Installation Procedure	5
Removing IMail Anti-Virus	8
Setting IMail Anti-Virus Options	8
Stopping and Starting IMail Anti-Virus	11
Viewing Files in the Mail Queue	11
Logging	12
Viewing Anti-Virus Messages in the SMTP Log	12
Informational Messages	13
Error Messages	13
Event Logging	14
Viewing Standard Logs	14
Alerting	14
Additional Alerts	15
Customizing Alert Messages	15
Editing Alert Strings	15
Editing Log Entries	16
Updating Virus Definitions	16
Configuring LiveUpdate to Check for Updates Automatically	17
Scan Engine's Web-Administrator	17

Setting Up IMail Anti-Virus

This document describes the IMail Anti-Virus solution. It includes information about installation, setting options, and viewing anti-virus events.

What is IMail Anti-Virus?

On today's networks, viruses and other destructive code are often sent as part of an e-mail message. IMail Anti-Virus works with your IMail Server software to find and repair infected messages before they get to your mail customers. IMail Anti-Virus, powered by Symantec's Anti-Virus™ Scan Engine 4.0 Server technology, formerly marketed as CarrierScan Server™, checks all incoming and outgoing mail for viruses, worms and trojan horses in all the major file types; including mobile code and compressed file formats. With our new solution, IMail administrators have the protection of Symantec's virus definitions and Scan Engine, which, of course, are kept up-to-date with Symantec's LiveUpdate™ technology to combat the latest known viruses.

IMail Anti-Virus can also discover new viruses by searching for general characteristics, or behaviors, of existing viruses. IMail Anti-Virus continuously scans each message, isolates infected files, and reports the results. You can set configuration options to determine what action to take when a virus is detected. And, IMail Anti-Virus software can even attempt to repair the infected message, delete the message, or bounce it so that the message is returned to the sender.

After installing IMail Anti-Virus and setting configuration options, you can get feedback on the virus scans from:

- SMTP Log — when a virus is detected, a log file entry is generated in the IMail SMTP Log.
- Alerts — In the configuration options, you can specify a mailbox to which an alert is sent (when a virus is detected).
- SMTP Queue — messages in the mail queue are identified as “already scanned” or “needs to be scanned.”

Frequently Asked Questions

This section covers some common questions about IMail Anti-Virus software.

What gets scanned?

IMail Anti-Virus is designed to work only with your IMail Server messages and attachments — it does not scan other files on your server.

Does it scan list server messages twice — incoming and outgoing?

Normally, a message destined for a mailing list would be scanned coming in; then, when the list server sent the message to the list, it would be scanned again. Since the scan does not need to be performed twice, messages sent to the list server will be scanned, but messages sent out by the list server will not.

Does the virus scan affect IMail Server processing speed?

Scanning mail messages for viruses adds approximately a 20 - 25% load on the mail server and can result in slightly slower processing.

How do I get updates to the virus definitions?

Getting virus definition updates is very easy. You can use the LiveUpdate™ application to get the latest virus definitions from Symantec. For information on using LiveUpdate, see “Updating Virus Definitions” on page 16.

Does a scan affect the processing order for other mail queue operations (list, forwarding, delivery rules etc.)?

All e-mails will be scanned, and the results of the scan can affect the processing order; for example, if the anti-virus software detects a virus and cannot repair the file, the file will be deleted, redirected, or, depending on the user settings, bounced. If a file is bounced, it will not be further processed for a list, forwarding, rules, or any other processing. If an infected message is cleaned, or it does not have a virus, the processing order is not affected.

Overview of Setup Tasks

This section provides a brief overview of the tasks that must be completed to successfully set up and install IMail Anti-Virus.

- 1 Check the prerequisites.
 - Check hardware and software requirements, and make sure your IMail Server software is at Version 7.04 or later. For more information, see “Installation Process” on page 4.
- 2 Install the software.
 - You must provide the IP address of the computer on which IMail Anti-Virus will be installed. IMail Anti-Virus, by default, runs on Port number 7777. If you want to use a different port, you should enter it during installation.
- 3 After installation, set options for how IMail Anti-Virus operates.
 - IMail Anti-Virus will run using the default configuration options. Make sure that **Enable virus scanning** is selected (see “Setting IMail Anti-Virus Options” on page 8). You can change any of the default settings.
- 4 Make sure IMail Anti-Virus is started. See “Stopping and Starting IMail Anti-Virus” on page 11 for more information.
- 5 Monitor anti-virus events by using the following:

- **SMTP Queue.**
See “Viewing Files in the Mail Queue” on page 11.
- **SMTP Log.**
See “Viewing Anti-Virus Messages in the SMTP Log” on page 12.
- **Windows Event Log.**
See “Event Logging” on page 14.
- **Alerts.**
See “Alerting” on page 14.

Installation Process

The IMail Anti-Virus CD contains:

- IMail Anti-Virus. This software can be installed on the IMail Server system (recommended for best performance) or on another computer in the local network.
- IMail Server Anti-Virus interface. This interface must be enabled in IMail Server, regardless of where IMail Anti-Virus is installed.

Note

IMail Server v7.04 or later is required for IMail Anti-Virus software (IMail Server 8.03 or later recommended).

Minimum System Requirements

Before you install IMail Anti-Virus, make sure the system on which you are installing meets the following requirements:

- IMail Server V.7.04 or later is required (IMail Server 8.03 or later recommended)
- Windows 2000 Server with Service Pack 2 or Windows 2000 Advanced Server with Service Pack 2
- IMail Anti-Virus and LiveUpdate™ require an Internet connection and Internet Explorer 6.0 or later.
- Pentium III 500 Mhz or higher
- 256+ MB of RAM
- 25 MB of hard disk space
- 1 NIC running TCP/IP with a static IP address
- 1 or more processors (depending on the mail traffic rates)

Before You Install

Consider the following:

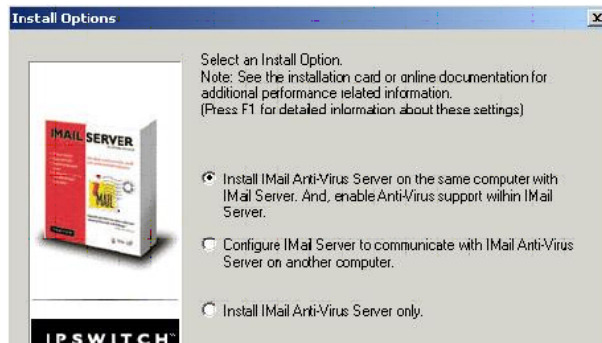
- Decide whether you will install IMail Anti-Virus on the same computer with the IMail Server software or on another computer in the local network. For best scanning performance, we recommend installing IMail Anti-Virus on the same computer with the IMail Server. If you **MUST** install IMail Anti-Virus on a separate computer, you still need to install IMail Anti-Virus on your IMail Server.

- If you do plan to install IMail Anti-Virus on a separate computer, you should install IMail Anti-Virus on that computer before running IMail Anti-Virus (Configure IMail Server) installation program option on the IMail Server.

Installation Procedure

To install IMail Anti-Virus software:

- 1 Log on to Windows NT or 2000 as System Administrator or to an account with system administrator permissions.
- 2 Back up your Windows registry. (Run *regedit.exe* and select **Export Registry File** from the **Registry** menu.)
- 3 Launch the IMail Anti-Virus executable file. (The installation process begins.) The *Welcome* screen appears. Read the text and click **Next**.
- 4 The *License Agreement* screen appears. Read the agreement and click **Yes** or **No**. Click **No** and the installation program will close. To accept the terms and to proceed with the installation, click **Yes**.
- 5 The *Install Options* screen appears. Select one of the following installation options and click **Next**.



Install Options

- **Install IMail Anti-Virus Server on the same computer with IMail Server. And, enable anti-virus support within IMail Server. (recommended).**

This installation option installs IMail Anti-Virus on the same computer where IMail Server is loaded. And, it enables you to access

anti-virus functionality from the IMail Server interface. If you do plan to install IMail Anti-Virus on a separate computer, you'll need to run this installation program on both computers. On each computer, during installation, you'll need to select one of the following options.

- **Enable Anti-Virus support within IMail Server.**

Select this option to enable the anti-virus components in your IMail Server, but not install IMail Anti-Virus on the same computer. This option will not install IMail Anti-Virus.

Note

This option only enables anti-virus support within IMail Server. You **MUST** separately install IMail Anti-Virus on the other computer. (When running the installation program from the other computer, select the third installation option.)

- **Install IMail Anti-Virus Server only.**

Select this option to install only IMail Anti-Virus on a separate computer from IMail Server. If you have not done so already, you will then need to enable the anti-virus features within IMail Server on a separate computer using the previous option. The third option will not automatically enable anti-virus support within IMail Server. To gain that functionality, you must run the installation program on the IMail Server computer and select the second installation option.

Note

The first and third installation options display only if the installation detects a Windows Server 2000 w/SP2 or greater OS. The primary reason to install IMail Anti-Virus on a separate computer from IMail Server is if your IMail Server is running on an NT Server.

-
- 6 The *Configure IMail Anti-Virus Server* screen appears. This screen contains the install-detected local IP address, port, and password for accessing Scan Engine's web-based administrator. For security purposes, you should change the "Admin" password, but we recommend keeping the default IP address and port settings. Change the Admin password and click **Next**.

- **IP Address.** Enter the IP address of the computer on which IMail Anti-Virus will be installed.
 - **Port.** Enter the port on which you want IMail Anti-Virus to run. The default port is 7777.
 - **Admin.** This password is used access to Symantec's Scan Engine web-based administrator. To protect your anti-virus application from unauthorized access, type a new password into this text field. Scan Engine's web-based administrator is located at: http://localhost:8004.
- 7 The *Select IMail Anti-Virus Server Folder* screen appears. Select the default destination folder or create a new entry. Click **Next**.
 - 8 The *License File* screen appears. Select the first option: “**Get the Symantec License File**” and click **Next**.

Note

The first time you install IMail Anti-Virus, you must register your product with Symantec. A completed registration activates your product's license.

- 9 Your browser launches and contacts Symantec. Symantec's *Licensing and Registration* page appears. Type your serial number and click **Submit**.

Note

Your serial number was provided to you at the time of purchase or delivered with your IMail Anti-Virus software.

- 10 Symantec's *Enter your Email Address and add any additional Serial Numbers* page appears. Type a valid e-mail address and click **Submit**.

Note

Symantec uses this address to send an e-mail message that contains an attached *.slf file.

(S p e c i a l N o t e): **The *.slf file is your product's license.**
Save the *.slf file for this and all future installations.

- 11 Symantec's *Confirm the following information* page appears. Make changes as needed and click **Submit**.

- 12 Symantec's *Thank you for using the licensing site* page appears.
- 13 Close your browser and wait for the e-mail from Symantec to be delivered. (Normally, the message is delivered within five minutes.)
- 14 The *License File* screen again appears.
If not already selected, select the second option: "**I have a Symantec License File**" and click **Next**.
- 15 The *Install License Wizard* screen appears. Click **Browse** and point to the location where you stored the *.slf file. When a valid *.slf file is detected, the install button will become enabled. Click **Install**.
- 16 The *Congratulations* screen appears. Click **Close**.
- 17 The *LiveUpdate* screen appears. Click **Next**.
- 18 LiveUpdate runs. When it's completed, click **Finish**.
- 19 The *IMail Server Update and IMail Anti-Virus Server Setup Complete* screen appears. Click **Finish**.
- 20 The product installation is completed. IMail Anti-Virus is protecting your IMail clients' messages.

Removing IMail Anti-Virus

Use the **Add/Remove Programs** applet in the Windows Control Panel.

The Uninstall program removes:

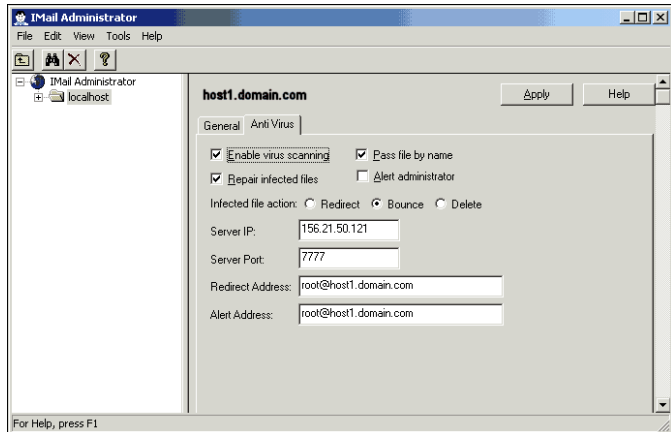
- The IMail Anti-Virus interface, which includes the Anti-Virus tab in IMail Administrator and the Anti-Virus Administration page in the IMail Web Messaging.
- The Symantec Scan Engine 4.0 Server and web administrator.

Setting IMail Anti-Virus Options

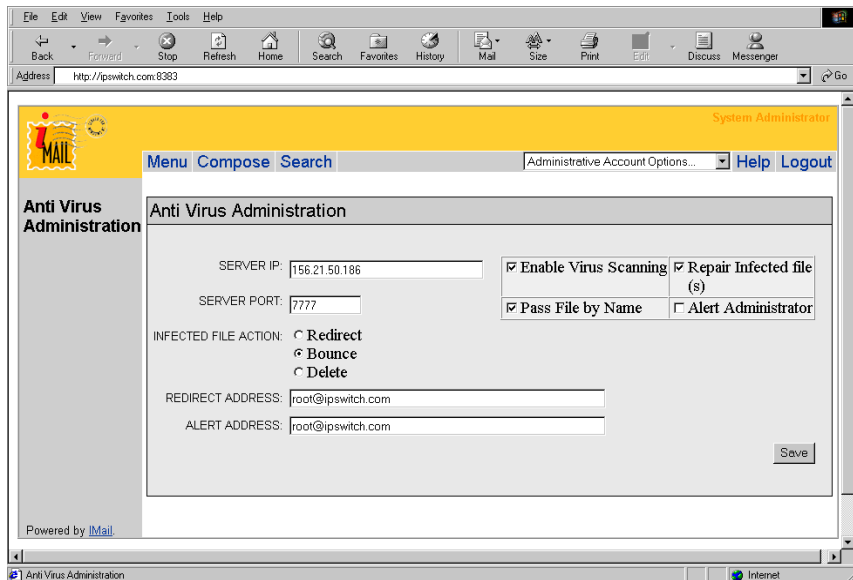
The anti-virus options let you:

- Enable or disable the anti-virus capability.
- Set the IP address and port number for the IMail Anti-Virus. Set the action to take when a virus is found in a mail message. The default action is "bounce."

- Set an e-mail address to which the anti-virus software will send an “alert” message when an infected file is found. You can set anti-virus options from two locations:
 - In the IMail Administrator, in the left panel, select **localhost**. In the right panel, select the Anti-Virus tab.



- In IMail Web Messaging, under Administrative Account Options..., select **Anti-Virus Administration**.



IMail Anti-Virus options:

- **Enable Virus Scanning.** This tells IMail Anti-Virus to begin scanning mail messages for viruses. If it is deselected, infected files WILL be delivered as normal.
- **Repair Infected Files.** Select this option if you want IMail Anti-Virus to attempt to repair a mail message which is infected. It does this by removing the infected portion and creating a new file containing the repaired message. The initial infected file will be deleted.
- **Pass File by Name.** If IMail Anti-Virus is installed on the same computer as IMail Server, we encourage you to select this option to increase performance.

Note

If you installed IMail Anti-Virus on a remote server, DO NOT select the **Pass File by Name** option.

Alert Administrator. Select this option to send an e-mail alert to the administrator when an infected file is found. One e-mail will be sent for each infected file, and will contain information such as who it is from, who it is to, the message ID, Subject, Virus Detected, and the Action taken. If you enable this option, be sure to enter an address in the Alert Address field.

Infected File Actions. Sometimes, IMail Anti-Virus software will be unable to repair an infected file. In such a case, it will take one of the following actions:

- **Bounce.** Select this option to send back non-repairable infected mail messages to the original sender. These messages are not delivered to any of the original recipients.
- **Redirect.** Select this option to redirect non-repairable infected messages to the recipient entered in the Redirect Address text box. These messages are not delivered to any of the original recipients.
- **Delete.** Select this option to delete infected messages from the spool directory. These messages are not delivered to any of the original recipients.

The Server IP and Server Port fields are, by default, filled in correctly during installation.

Note

The **Server IP** address and the **Server Port** in this dialog box must match the “Bindaddress” and the “Port” set in the *symscan.cfg* file. If you want to change the address or port, you must change them in both places.

Server Port. The port on which you want IMail Anti-Virus to run. The default port is 7777.

Redirect Address. If you set the Infected File Action to Redirect, enter an e-mail address to which infected messages are sent.

Alert Address. Type an address here if you have enabled the Alert Administrator option. This address will receive an e-mail containing details if an infected file is found.

To save your selections or changes, click **Apply**.

Stopping and Starting IMail Anti-Virus

You can stop and start IMail Anti-Virus by using the Windows Services interface.

On the desktop, right-click the **My Computer** icon and select **Manage**. In the **Computer Management** window, expand the **Services and Applications**, and select **Services**. Look for the service named: Symantec Scan Engine 4.0 Server

Note

A second service (Symantec Watchdog Server) monitors whether anti-virus software (Symantec Scan Engine 4.0 Server) is running.

Viewing Files in the Mail Queue

An anti-virus entry type has been added to the queue file for SMTP32. This entry type identifies the status of the virus scan for a particular message. The entry will have a V in the first column,

followed by a 1 or a 0. The following chart displays the possible queue entries for the anti-virus scan.

V1	Message has already been scanned by the anti-virus software.
V0	Message needs to be scanned.
No entry	Message needs to be scanned.

List Server Interaction

Because IMail Anti-Virus software scans all incoming and outgoing mail messages, special provisions had to be made concerning the list server. Normally, the anti-virus software scans a list server message twice. Once when the message came in, and, again, when the list server sent the message to the list. And, because messages are scanned prior to being processed by the list server, they must be scanned when sent by the list server. Therefore, all messages destined for a list server are automatically marked (in the mail queue) as scanned.

Logging

Log messages that report status or errors from the IMail Anti-Virus software can be viewed in either of two places: SMTP Log or Windows Event Log

Viewing Anti-Virus Messages in the SMTP Log

Some messages from the IMail Anti-Virus software are recorded in IMail Server's SMTP log. These messages record events.

Examples of these events include: virus is detected, actions taken, errors, and the times when IMail Anti-Virus becomes unavailable.

Note

Other messages from IMail Anti-Virus are recorded in the Windows Event Log. For more information about anti-virus messages, see "Event Logging" on page 14.

To view the SMTP log:

From the IMail Administrator, expand the **localhost** folder, expand the **Services** folder, then select **SysLog**. The right panel shows the logs.

Messages from the SMTP service (along with messages from other services) are logged to a file named *sysMMDD.txt*, where *MM* is the

month and *DD* is the date. In this log, you may see two types of messages from the IMail Anti-Virus software: informational messages and error messages.

Informational Messages

When a virus is detected, the IMail Anti-Virus software writes a message to the SMTP log stating what action was taken.

An example of an Informational Message is:

```
08:23 10:27 SMTP-(000001DE) virus detected, Virus repaired, virus data = EICAR test string
08:23 10:36 SMTP- (000001D6) Virus detected, Not repaired, Redirected, Virus data = EICAR test string
08:23 10:37 SMTP-(000000E8) Virus detected, Not repaired, Message deleted, Virus data = EICAR test string
```

Error Messages

When there's a problem with the connection to IMail Anti-Virus or a with a scan, an error message is written to the SMTP log. When IMail Anti-Virus scans a file using Scan Engine it returns a code. If this code is not 0, -1 or -3, it is reported as an error in the log.

An example of this log is:

```
08:23 10:39 SMTP-(00000164) Failed to initialize virus scanner, Code=1 (see codes below)
08:23 16:28 SMTP-(0000012E) Error from Virus scan server, Code=1 (see codes below)
08:23 16:28 SMTP-(0000012E) Error -Virus scan call generated general fault
08:23 16:28 SMTP-(0000012E) Virus scan initiation caused general fault
```

An error message may reference one of these error codes:

Error Code	Description
1	SCSCANFILE_FAIL_CONNECT Failed to connect to IMail Anti-Virus
2	SCSCANFILE_FAIL_INPUTFILE A problem was encountered reading the file to be scanned.
3	SCSCANFILE_FAIL_ABORTED The scan was aborted abnormally.
4	SCSCANFILE_INVALID_PARAM Function was called with an invalid parameter.
5	SCSCANFILE_FAIL_RECV_FILE Error occurred when attempting to receive repaired file.
6	SCSCANFILE_FAIL_MEMORY A memory allocation error has occurred.

Error Code	Description
7	SCSCANFILE_FAIL_FILE_ACCESS The server couldn't access the file to be scanned. This error usually occurs for LOCAL scans when the file permissions are wrong. This error can also occur when the API encounters a problem while writing repaired file data that was received from the scan engine to the output file.
8	SCSCANFILE_FAIL_EXTRACTTIME
9	SCSCANFILE_FAIL_REPAIRFILE
10	SCSCANFILE_ERROR_SCANNINGFILE An internal server error occurred while the scan engine was attempting to repair the file.
15	SCSCANFILE_ABORT_NO_AV_SCANNING_LICENSE No valid license for antivirus scanning functionality is installed.

Event Logging

IMail Anti-Virus logs error messages and files to the Windows Event Log. However, logging is not enabled by default. If you want to log error messages, you must first enable logging. To do this, edit the *symscan.cfg* file located in the *C:SYMCSan* directory. This file contains the configuration options for Symantec's IMail Anti-Virus.

To Enable Logging (Defaults to the Windows Event Log):

- 1 Open the *symscan.cfg* file and scroll to the **Logging** section.
- 2 Select the types of messages that you want to log and change their value from 0 to 1.
- 3 From the **File** menu, Select **Save**.

Viewing Standard Logs

The NT Event Log contains IMail Anti-Virus logs. To access the Windows Application Event Log:

- 1 Open the Event Viewer.
- 2 Under Log, click **Application**.
- 3 Click any IMail Anti-Virus event listed in the Application Log to view that log entry.

Alerting

If you select the **Alert Administrator** option, IMail Anti-Virus sends an e-mail alert to the administrator in the event of an infected file. One e-mail will be sent for each infected file, and it will contain

information such as who it is from, who it is to, the message ID, Subject, Virus Detected, and the Action taken. If you enable this option, be sure to enter an address in the **Alert Address** field.

For information about setting this option, see “Setting IMail Anti-Virus Options” on page 8.

Additional Alerts

IMail Anti-Virus can be configured to send additional SMTP e-mail alerts. Primary and backup alert servers (SMTP servers) can be specified for redundancy.

The SMTP alerts for IMail Anti-Virus are straightforward. This section discusses IMail Anti-Virus alerts and provides information on customizing alert messages.

Customizing Alert Messages

Some of IMail Anti-Virus alert messages can be customized by editing the message string file. The default location is `<driveletter>:\SYMCSan\symcsmg.dat`, where `<driveletter>` is the drive letter on which Windows NT or 2000 is installed.

Double-byte characters are supported for the IMail Anti-Virus message string text. For each message string file entry, the text that follows the space after the message number and before the `***` can be edited.

Editing Alert Strings

The following table describes each message string file entry used in generating IMail Anti-Virus alerts.

No.	Default message text	Usage in alert subsystem
1001	IMail Anti-Virus IP address:<IPaddress>	The IP address of IMail Anti-Virus that is the subject of the alert
1002	IMail Anti-Virus port number:<portnumber>	The port number of IMail Anti-Virus that is the subject of the alert
1003	IMail Anti-Virus virus fingerprint date:<virus fingerprintdate>	The date the virus definitions that are the subject of the alert were created (for virus update or update error)
1004	IMail Anti-Virus threshold queue size:<queuesize>	The threshold queue size for IMail Anti-Virus that is the subject of the alert
1005	IMail Anti-Virus number of queued items:<queueditems>	The number of queued scan requests for IMail Anti-Virus at the time of the reported event
1006	Date/time of event:<date/time>	The date and time of occurrence for the reported event (IMail Anti-Virus crash, start-up, shutdown, etc.)
1007	System uptime (in seconds):<time>	The amount of time (at the time of the alert) that IMail Anti-Virus has been running since the last crash or since start-up

1008	IMail Anti-Virus Crash Alert	Subject of IMail Anti-Virus Crash Alert
1009	IMail Anti-Virus crashed	Message body text for IMail Anti-Virus Crash Alert
1010	IMail Anti-Virus Startup Alert	Subject of IMail Anti-Virus Start-up Alert
1011	IMail Anti-Virus has just started up.	Message body text for IMail Anti-Virus Start-up Alert
1012	IMail Anti-Virus shutdown alert	Subject of IMail Anti-Virus Shutdown Alert
1013	IMail Anti-Virus has been manually shut down.	Message body text for IMail Anti-Virus Shutdown Alert
1014	IMail Anti-Virus Definition Update Alert	Subject of IMail Anti-Virus Definition Update Alert
1015	IMail Anti-Virus has updated its virus definitions.	Message body text for IMail Anti-Virus Definition Update Alert
1016	IMail Anti-Virus Queue Overflow	Subject of IMail Anti-Virus Load Exceeded Alert
1017	IMail Anti-Virus queue is backing up due to a large number of requests.	Message body text for IMail Anti-Virus Load Exceeded Alert
1018	IMail Anti-Virus Definition Error Alert	Subject of IMail Anti-Virus Definition Update Error Alert
1019	There was an error loading IMail Anti-Virus virus definitions. All scanning will be disabled.	Message body text for IMail Anti-Virus Definition Update Error Alert

Editing Log Entries

The 4000-series message strings are used in log entries (when appropriate logging is enabled). These message strings are described in the following table.

No.	Default message text	Usage
4000	A virus or other malicious code has been detected.<filename:virusname>	Log entry text when a virus is detected (appropriate logging must be enabled)
4001	A file has been received and scanned.<filename>	Log entry text when a file is scanned (LOGFileScanAlertEnable must be activated to induce logging of every file scanned)
4002	Error trying to send an SMTP alert.	Log entry text used if SMTP alerting fails for some reason, for example, the SMTP server was unreachable

Updating Virus Definitions

The LiveUpdate feature ensures that you are not at risk of infection by newly discovered viruses. IMail Anti-Virus can be updated with the latest virus definitions without any interruption of virus scanning.

Updated virus definitions files, which contain the necessary information to detect and eliminate viruses, are supplied by Symantec at least every week and whenever a new virus threat is discovered. When new virus definitions are available, the LiveUpdate technology can automatically download the proper files and install them in the proper location (if you configure this LiveUpdate option).

To start the LiveUpdate utility:

- From the **Start** menu, select **Programs -> IMail -> LiveUpdate**.

A LiveUpdate client, *cslive.exe*, is installed with IMail Anti-Virus. You should not have to edit the LiveUpdate configuration unless you have set up your own LiveUpdate server.

For more information on specific settings and troubleshooting, see the LiveUpdate Help file (*S32luhp.hlp*) located in the same directory folder. You can also view the PDF file, *luadmin.pdf*, located in the IMail top directory.

Configuring LiveUpdate to Check for Updates Automatically

You can schedule LiveUpdate to occur automatically at a specified time to ensure that IMail Anti-Virus always has the most current virus definitions. The *cslive.exe* client can be run from the command line to update virus definitions for IMail Anti-Virus.

To run the LiveUpdate client:

Type one of the following commands:

- `cslive /silent` to run LiveUpdate in silent mode (no prompting or display indicator).
- `cslive.exe` to run LiveUpdate and display a progress indicator.

LiveUpdate should be scheduled to run periodically (at least weekly) by using the Windows NT at command.

An example of this command is:

```
at 02:00 every:M \SYMCSan\cslive /silent
```

This command runs LiveUpdate every Monday at 2:00 AM with no user intervention (*/silent*).

Scan Engine's Web-Administrator

Access to Symantec's Scan Engine protocols and administration settings can be accessed through Scan Engine's Web-Administrator. You'll find this application at: `http://localhost:8004`. This administrator is installed with its own separate help system.

Be aware Ipswitch recommends you accept the native protocols that were set during the installation process and not access this administrator application.

