

---

# IMail Anti-Virus

---

## Setup Guide

Software Version V1.0

---

**Ipswitch, Inc.**

Ipswitch, Inc.  
81 Hartwell Ave  
Lexington, MA 02421

**Phone:** 781-676-5700  
**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 © 1995-2001 by Ipswitch, Inc. All rights reserved. IMail, the IMail logo, WhatsUp, the WhatsUp logo, WS\_FTP, the WS\_FTP logos, 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.

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

# Contents

<b>Setting Up IMail Anti-Virus</b> .....	<b>1</b>
What is IMail Anti-Virus? .....	1
Frequently Asked Questions .....	2
Overview of Setup Tasks .....	3
Installing .....	4
Requirements for the Anti-Virus Server .....	4
Before You Install .....	5
Installation Procedure .....	5
Removing IMail Anti-Virus .....	7
Setting Anti-Virus Options .....	7
Stopping and Starting the Anti-Virus Server .....	10
Viewing Files in the Mail Queue .....	11
Logging .....	11
Viewing Anti-Virus Messages in the SMTP Log .....	12
Informational Messages .....	12
Error Messages .....	13
Event Logging .....	13
Viewing standard logs .....	14
Alerting .....	14
Additional Alerts .....	14
Customizing alert messages .....	14
Editing alert strings .....	15
Editing log entries .....	16
Updating Anti-Virus Rules .....	16
Configuring LiveUpdate to check for updates automatically .....	17
<b>Appendix A: Editing the Configuration File</b> .....	<b>19</b>
Specifying the bind address .....	20
Specifying the IMail Anti-Virus Server port number .....	21
Specifying the temporary directory location .....	21
Selecting the number of scan threads .....	21
Selecting the Bloodhound sensitivity level .....	22
Specifying the message string file location and file name .....	23
Specifying the log file location .....	23
Specifying the alert interval .....	24
Specifying the threshold number of queued requests .....	24
Specifying what to log .....	25
Activating SMTP alerting .....	27
Specifying which file types to scan .....	28



---

# Setting Up IMail Anti-Virus

This document describes the IMail Server Anti-Virus solution and how to install it, set options, and view 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. The IMail Anti-Virus server, powered by Symantec's CarrierScan technology, checks all incoming and outgoing mail for viruses, worms, trojan horses and other destructive code. With this solution, IMail administrators have the protection of Symantec's anti-virus rules database, which is continuously updated to combat the latest viruses.

The Anti-Virus server can also discover new viruses by searching for general characteristics, or behaviors, of existing viruses.

The Anti-Virus server 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. The Anti-Virus software can 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 Frequently Asked Question about the IMail Anti-Virus software.

### **What gets scanned?**

The IMail Anti-Virus server works 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.

To distribute the processing load, you can install the IMail Anti-Virus server on a separate server from the IMail Server system, but this should only be necessary for installations with a large number of mail users (for example, 4000 + users).

### **How do I get Updates to the anti-virus rules?**

You can use the LiveUpdate application to get the latest anti-virus rules from Symantec. For information on using LiveUpdate, see “Updating Anti-Virus Rules” 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 it cannot repair the file, the file will be deleted, redirected, or bounced, depending on the user settings. In this case, the file will not be further processed for a list, forwarding, rules, or any other processing. If an infected message is cleaned, or does not have a virus, the processing order is not affected.

---

## Overview of Setup Tasks

This section provides an overview of the tasks you must complete to set up the Anti-Virus Server. The rest of this manual describes these tasks in detail.

1 Check the prerequisites.

Check hardware and software requirements, and make sure your IMail Server software is at Version 7.0 or later. For more information, see “Installing” on page 4.

2 Install the software.

You must provide the IP address of the computer on which the IMail Anti-Virus server will be installed. The Anti-Virus server will run on Port number 7777, by default. If you want to use a different port, you should enter it during installation.

3 Set options for how the anti-virus server operates.

After installing IMail Anti-Virus, the anti-virus server will run using the default configuration options. Make sure that **Enable virus scanning** is selected (see “Setting Anti-Virus Options” on page 7). You can change any of the default settings.

4 Make sure the anti-virus server is started. See “Stopping and Starting the Anti-Virus Server” on page 10 for more information.

5 You can 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 13.
- Alerts. See “Alerting” on page 14.

---

## Installing

The IMail Server Anti-Virus CD contains:

- IMail Anti-Virus server, which scans mail for viruses. This server can be installed on the IMail Server system, which is recommended for best performance; or on another computer in the local network.
- IMail Server Anti-Virus interface, which presents the configuration options for the IMail Anti-Virus server. This interface must be installed on the IMail Server system, regardless of where the IMail Anti-Virus server is installed.

---

### Note

IMail Server V7.04 or later is a prerequisite for the IMail Anti-Virus software. If necessary, the IMail Anti-Virus installation program will update your IMail Server software to Version 7.04. In order to do this, you must have IMail Server V7.0 or later software already installed. This installation program will NOT upgrade a pre-V7.0 installation. If you currently have a version of IMail Server later than version 7.04, this installation will not downgrade your system. In such a case, you will retain the higher version and only the IMail Anti-Virus Server will be installed.

---

### Requirements for the Anti-Virus Server

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

- Windows NT Server 4.0 with Service Pack 4 or higher installed or Windows 2000 Server
- The IMail Anti-Virus server and LiveUpdate require Internet Explorer 4.71.1712.6 or later be installed.
- Pentium III 500 Mhz or higher
- 256–512MB of RAM
- 8+ GB of hard disk space
- 1 or more network cards
- 1 or more processors (depending on the mail traffic rates)

## Before You Install

Before you run the IMail Anti-Virus installation program, consider the following:

- Decide whether you will install the IMail Anti-Virus server on the same computer with the IMail Server software or on another computer in the local network.

For best scanning performance, we recommend that you install the IMail Anti-Virus server on the same computer with the IMail Server software. If your IMail Server software supports a large number of users (for example, 4000 +), you may get better overall performance by installing the IMail Anti-Virus server on a separate computer.

If you will install the IMail Anti-Virus server on a separate computer, note that you will still need to run the IMail Anti-Virus installation program on your IMail Server system.

- Order of installation: If you plan to install the IMail Anti-Virus server on a separate computer from the IMail Server, you should complete that installation before you run the IMail Anti-Virus installation program on the IMail Server system.

## Installation Procedure

To install the 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 Do one of the following:
  - If you purchased an IMail Anti-Virus CD-ROM, insert it in the CD\_ROM drive. If the installation program does not run automatically, select **Run** from the **File** menu, and enter the CD\_ROM path followed by *setup.exe*.
  - If you downloaded IMail Anti-Virus from our web site, click on the downloaded file to start the installation.

#### 4 Select the Components to Install.

To install the IMail Anti-Virus server on the same computer with your IMail Server software (and upgrade IMail Server, if necessary), select the option:

- **Install IMail Anti-Virus Server and enable Anti-Virus support within IMail Server (recommended).**

If you plan to install the IMail Anti-Virus server on a separate computer, you need to run this installation program on both computers, each time selecting one of the following options:

- **Enable Anti-Virus support within IMail Server.** Select this option to upgrade your current IMail Server program to include anti-virus components, but not install the IMail Anti-Virus server. If you select this option, you will then need to install the IMail Anti-Virus server on a separate computer using the next option.
- **Install IMail Anti-Virus Server only.** Select this option to install only the IMail Anti-Virus Server on a separate computer from IMail Server. If you have not done so already, you will then need to upgrade IMail Server to 7.04 or later on a separate computer using the previous option.

---

#### Note

The only reason to install IMail Anti-Virus on a separate computer from IMail Server is to reduce the load on heavily stressed machines (heavy traffic and over 4,000 users).

---

---

#### Note

If you currently have a version of IMail Server later than version 7.04, this installation will not downgrade your system. In such a case, you will retain the higher version and only the IMail Anti-Virus Server will be installed.

---

- #### 5 Update Virus Definitions.
- IMail Anti-Virus Server employs Symantec's LiveUpdate utility to update virus definitions. LiveUpdate connects to Symantec's site and determines if the software that you are running requires an update. If the answer is yes, then the virus definition update is copied to your system.

It is imperative that you run LiveUpdate on your newly installed anti-virus software, because no virus definitions are installed by default. We recommend that you run this utility during the installation process.

LiveUpdate runs at the end of the IMail Anti-Virus installation. If it is necessary to reboot your computer, LiveUpdate will run automatically when your computer is restarted.

- 6 **Configuration.** Enter the **IP Address** of the computer on which the IMail Anti-Virus server will be installed.

Enter the **Port** on which you want the IMail Anti-Virus server to run. The default port is 7777. If you do not enter a port number in this field, the anti-virus server will run on the default port.

- 7 If prompted, restart your system when the setup is complete.  
If you selected to run the LiveUpdate, it runs after the reboot.

---

## Removing IMail Anti-Virus

To remove 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 anti-virus server (Symantec CarrierScan Server).

---

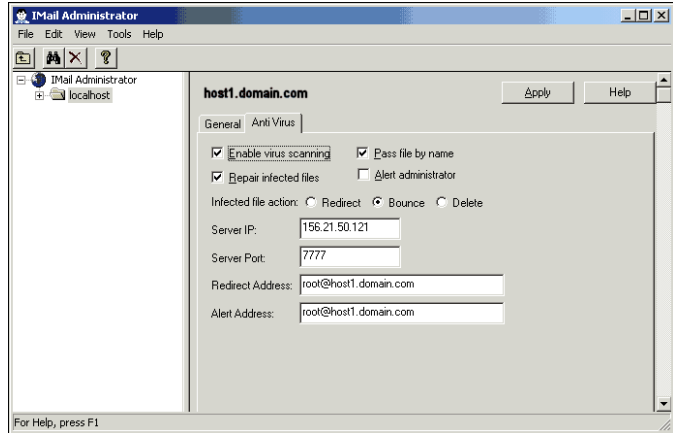
## Setting Anti-Virus Options

The anti-virus options let you:

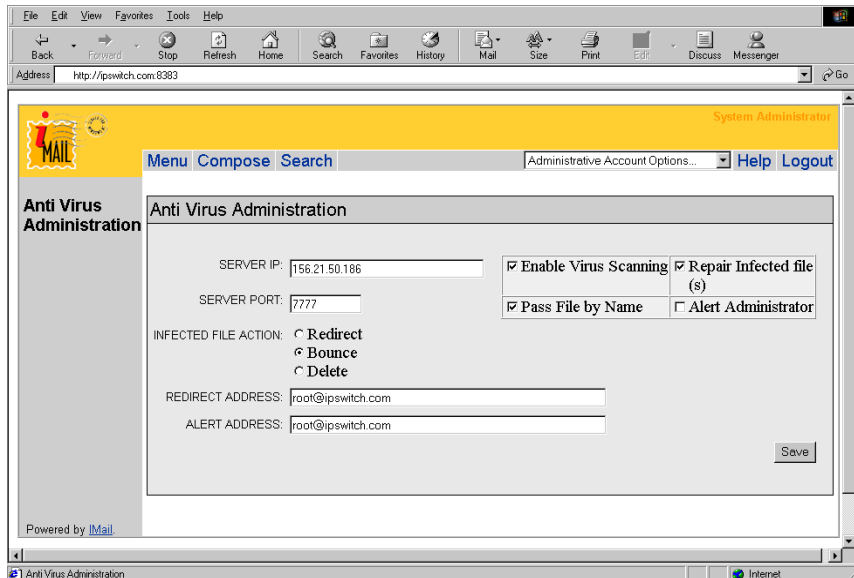
- Enable or disable the Anti-Virus capability.
- Set the IP address and port number for the Anti-Virus server.
- Set the action to take when a virus is found in a mail message. The default action is “bounce,” which means the infected mail message will be returned to the sender.
- Set an e-mail address 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**.



To set any of these anti-virus options:

- 1 Select **Enable Virus Scanning**. This tells the anti-virus server to begin scanning mail messages for viruses. If it is deselected, infected files WILL be delivered as normal.
- 2 Enable the optional settings as described below:

**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 the IMail Anti-Virus server is installed on the same computer as IMail Server, we encourage you to select this option to increase performance.

---

**Note**

If you installed the IMail Anti-Virus server 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.

- 3 Select one of the following **Infected File Actions**. Sometimes, the 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 bounce the infected mail message (that could not be repaired) back to the sender, without delivering the messages to the original recipients.

**Redirect.** Select this option to redirect the infected message (that could not be repaired) to the recipient entered into the Redirect Address field. The message is not delivered to any of the original recipients.

**Delete.** Select this option to delete the infected message from the pool directory. The message is not delivered to any recipient.

- 4 Make entries in the following fields. The **Server IP** and **Server Port** fields should be filled in by default if you entered the information 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 *symcscan.cfg* file. If you want to change the address or port, you must change them in both places. For information on making this change in the configuration files, see “Appendix A: Editing the Configuration File” on page 19.

---

**Server IP.** The IP address of the computer on which IMail Anti-Virus server is installed.

**Server Port.** The port on which you want the IMail Anti-Virus server 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.** Enter 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.

- 5 Click **Apply** to save your changes.

---

#### Note

You can set additional anti-virus options by editing the configuration file associated with the scan server. For more information, see “Appendix A: Editing the Configuration File” on page 19.

---

---

## Stopping and Starting the Anti-Virus Server

You can stop and start the IMail Anti-Virus server by using the Windows NT or Windows 2000 Services interface.

In Windows NT, open the **Control Panel**, select the **Services** icon and look for the service named: IMail Anti-Virus Server.

In Windows 2000, 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 CarrierScan Server

---

### Note

A second service (Symantec Watchdog Server) monitors whether the anti-virus server (Symantec CarrierScan 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 the 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 would scan a list server message twice, once when the message came in, and another time when the list server sent the message to the list.

Because messages are scanned prior to being processed by the list server, they do need to 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

There are two places where you can view log messages that report status or errors from the IMail Anti-Virus software.

- SMTP Log
- Windows Event Log

The following sections describe what is displayed by each 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, such as when a virus is detected and the action taken, and errors, such as if the IMail Anti-Virus server becomes unavailable.

---

### Note

Other messages from the IMail Anti-Virus server are recorded in the Windows Event Log. For more information about anti-virus messages, see "Event Logging" on page 13.

---

To view the SMTP log:

In 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. For example:

```
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 a problem exists with the connection to the IMail Anti-Virus server, or a with a scan, an error message is written to the SMTP log.

For example:

```
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	Failed to connect to IMail Anti-Virus
2	A problem was encountered reading the file to be scanned.
3	The scan was aborted abnormally.
4	Function was called with an invalid parameter.
5	Error occurred when attempting to receive repaired file.
6	Memory allocation error.
7	Server could not access the file to be scanned. This error usually occurs for <i>local</i> scans when file permission are wrong or when the file is not in the path specified in the LocalFileScanDir parameter on the server.

---

## Event Logging

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

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

- 1 Open the *symcscan.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 Server logs. To access the NT Application Event Log:

- 1 Open the Event Viewer.
- 2 Under Log, click **Application**.
- 3 Click any IMail Anti-Virus Server 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 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 Anti-Virus Options” on page 7.

### Additional Alerts

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

### Customizing alert messages

Some of the IMail Anti-Virus Server 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 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 Server alerts.

No.	Default message text	Usage in alert subsystem
1001	IMail Anti-Virus Server IP address:<IPaddress>	The IP address of the IMail Anti-Virus Server that is the subject of the alert
1002	IMail Anti-Virus Server port number:<portnumber>	The port number of the IMail Anti-Virus Server that is the subject of the alert
1003	IMail Anti-Virus Server 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 Server threshold queue size:<queuesize>	The threshold queue size for the IMail Anti-Virus Server that is the subject of the alert
1005	IMail Anti-Virus Server number of queued items:<queueditems>	The number of queued scan requests for the IMail Anti-Virus Server 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 Server 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 Server has been running since the last crash or since start-up
1008	IMail Anti-Virus Server Crash Alert	Subject of IMail Anti-Virus Server Crash Alert
1009	The IMail Anti-Virus Server crashed	Message body text for IMail Anti-Virus Crash Alert
1010	IMail Anti-Virus Server Startup Alert	Subject of IMail Anti-Virus Server Start-up Alert
1011	The IMail Anti-Virus Server has just started up.	Message body text for IMail Anti-Virus Start-up Alert
1012	IMail Anti-Virus Server shutdown alert	Subject of IMail Anti-Virus Server Shutdown Alert
1013	The IMail Anti-Virus Server has been manually shut down.	Message body text for IMail Anti-Virus Shutdown Alert
1014	IMail Anti-Virus Server Virus Definition Update Alert	Subject of IMail Anti-Virus Server Virus Definition Update Alert
1015	The IMail Anti-Virus Server has updated its virus definitions.	Message body text for IMail Anti-Virus Server Virus Definition Update Alert
1016	IMail Anti-Virus Server Queue Overflow	Subject of IMail Anti-Virus Server Load Exceeded Alert
1017	The IMail Anti-Virus Server queue is backing up due to a large number of requests.	Message body text for IMail Anti-Virus Server Load Exceeded Alert
1018	IMail Anti-Virus Server Virus Definition Error Alert	Subject of IMail Anti-Virus Server Virus Definition Update Error Alert
1019	There was an error loading the IMail Anti-Virus Server virus definitions. All scanning will be disabled.	Message body text for IMail Anti-Virus Server 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.

For more information, see “Specifying what to log” on page 25.

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 Anti-Virus Rules

The LiveUpdate feature ensures that you are not at risk of infection by newly discovered viruses. A LiveUpdate client is installed with IMail Anti-Virus Server. IMail Anti-Virus Server 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 Server. 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 Server 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 Server.

### To run the LiveUpdate client:

- Type one of the following commands:
  - `cslive.exe -s` 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. For example:

```
at 02:00 every:M \SYMCSan\cslive.exe -s
```

This command runs LiveUpdate every Monday at 2:00 AM with no user intervention (-s).



---

## Appendix A: Editing the Configuration File

At installation, you are prompted to supply certain information to configure IMail Anti-Virus Server. Following installation, you can change these and other settings by editing the configuration file, *symcscan.cfg*. This section provides information on the configuration options.

Two of the options in this file are initially set by the installation program: the BindAddress (IP Address of the installation machine) and Port number (on which the Anti-Virus Server runs).

Additional configuration options not presented during installation include:

- Specifying the temporary directory location
- Selecting the number of scan threads
- Setting the Bloodhound sensitivity level (looks for new or unknown viruses)
- Message string file name and location
- Location for IMail Anti-Virus Server log files
- Specifying the alert interval
- Specifying the threshold number of queued requests
- Specifying what to log (in the Windows Event Log)
- Activating SMTP Alerting
- Types of files scanned by IMail Anti-Virus Server

### To edit the IMail Anti-Virus Server configuration file:

- 1 Locate the IMail Anti-Virus Server configuration file.

The default location for the configuration file is

<driveletter>:\SYMCScan\symcscan.cfg, where <driveletter> is the drive letter on which Windows NT or 2000 is installed.

- 2 Open the configuration file with a text editor.
- 3 Make the necessary changes to the configuration file.  
The following sections describe the configuration options.
- 4 Save the changes to the file.
- 5 Stop and restart the IMail Anti-Virus server (See “Stopping and Starting the Anti-Virus Server” on page 10.)

### Specifying the bind address

The bind address is the IP address on which IMail Anti-Virus Server listens. This IP address is generally the address of the computer on which IMail Anti-Virus Server is installed. In some cases, computers are configured to have multiple IP addresses, so this setting lets you specify a particular address.

---

#### Note

The “Bindaddress” set in the *symcscan.cfg* file must match the **Server IP** address in the IMail Administrator Anti-Virus dialog box. If you want to change the address, you must change it in both places. For information on making this change in the Anti-Virus dialog box, see “Setting Anti-Virus Options” on page 7.

---

To change the bind address, you can edit the configuration file.

---

#### Note

For this setting, you can use 127.0.0.1, which is a special address called the loopback interface. If you use this address, only clients running on the same computer as IMail Anti-Virus Server can connect to IMail Anti-Virus Server.

---

### To specify a bind address in the configuration file:

- At Bindaddress=, type the IP address on which IMail Anti-Virus Server listens.

## Specifying the IMail Anti-Virus Server port number

IMail Server passes files to be scanned for viruses to IMail Anti-Virus Server via a TCP/IP port number. This port number must be exclusive to IMail Anti-Virus Server. The default port number is 7777. If you change the IMail Anti-Virus port number, select a port number greater than 1024 not in use by any other program or service.

---

### Note

The “Port” set in the *symscan.cfg* file must match the **Server Port** in the IMail Administrator Anti-Virus dialog box. If you want to change the port, you must change it in both places. For information on making this change in the Anti-Virus dialog box, see “Setting Anti-Virus Options” on page 7.

---

To change the port number in the configuration file:

- At Port=, replace the existing port number with the new number.

## Specifying the temporary directory location

Files must be stored in their entirety in a temporary directory for virus scanning. To support sites with large, specialized disk configuration, the location of this temporary directory can be specified. The disk space required for this directory varies with the volume of files to be scanned.

IMail Anti-Virus Server performance is dependent on this directory accommodating potentially large numbers of large files during periods of peak usage.

The default location is C:\TEMP. The temporary directory specified for IMail Anti-Virus Server must already exist on the computer.

To specify a different location for the temporary directory in the configuration file:

- At TempDir=, replace the existing path with the new path.

## Selecting the number of scan threads

Multiple files can be scanned concurrently by IMail Anti-Virus Server. You can select the number of available threads for concurrent scanning. The default number of threads is 5.

Usage may be the only method for determining the optimal setting for the number of available threads. Performance is dependent on scan volume, the number of client applications making requests to IMail Anti-Virus Server, available memory and disk space, and the selected number of scanning threads.

---

#### **Note**

When the number of scan requests exceeds the number of scan threads available, scan requests are queued until a thread becomes available. The threshold number of queued requests is configured for IMail Anti-Virus Server, above which IMail Anti-Virus Server is at maximum load. IMail Anti-Virus Server can be configured to log instances when the load is exceeded, and to send alerts at a prescribed interval.

---

#### **To change the number of scan threads in the configuration file:**

- At ScanThreads=, replace the existing number of threads with the new number.

#### **Selecting the Bloodhound sensitivity level**

To supplement detection of virus infections by virus signature, IMail Anti-Virus Server includes Symantec's patented Bloodhound technology, which heuristically detects new or unknown viruses, based on certain characteristics generally exhibited by viruses. The sensitivity of the Bloodhound technology can be adjusted. Increasing the sensitivity may increase the likelihood of an occasional false positive.

The default Bloodhound sensitivity setting is 2 (medium). You can select from a range of values from 0 to 3, where 0 is off; 1, low; 2, medium; and 3, high.

#### **To change the Bloodhound sensitivity setting in the configuration file:**

- At BloodhoundLevel=, replace the existing setting with the new setting.

## **Specifying the message string file location and file name**

Message text for IMail Anti-Virus Server's alert messages and SMTP insert messages is contained in an ASCII text file. You can change the location and file name for this file by editing the configuration file. The default location for is <driveletter>:\SYMCSan\symcsmg.dat, where <driveletter> is the drive on which Windows NT or 2000 is installed. If you change the directory structure for the string file, the specified location must exist on the machine.

IMail Anti-Virus Server alert messages may be customized by editing this string file.

For more information, see "Alerting" on page 14.

### **To change the path and file name for the message string file in the configuration file:**

- At StringFile=, replace the existing path and file name with a new path and file name.

## **Specifying the log file location**

IMail Anti-Virus Server maintains standard logs that contain, for example, information on start-up, shutdown, system crashes, and virus definition updates. You can select the standard information that is logged by IMail Anti-Virus Server. For more information, see "Specifying what to log" on page 25.

You can change the location for the IMail Anti-Virus log files by editing the configuration file. The file names for the log files cannot be changed. The NT Event log contains the logs for Windows NT and Windows 2000. Keep in mind that the disk space required for the log files varies with scan volume and associated activity; the specified location must accommodate these files. The directory structure specified for the log file location must exist on the computer.

### **To specify a different location for IMail Anti-Virus Server log files in the configuration file:**

- At LogDir=, replace the existing location with the new location.

## Specifying the alert interval

IMail Anti-Virus Server can be configured to send alerts when a specified maximum load is exceeded. You can specify the length of the interval, in minutes, between IMail Anti-Virus Server alerts generated to indicate that maximum load has been exceeded. The default setting is 5 minutes. If you are changing the alert interval, take into consideration that IMail Anti-Virus Server may remain at maximum load for a period of time. Select an interval that will be informative but will not result in a flood of SMTP messages or log entries during that period. For alerts to be generated, you must also activate the appropriate SMTP alerts.

For more information, see “Activating SMTP alerting” on page 27.

---

### Note

The maximum load is exceeded when the number of requests to IMail Anti-Virus Server exceeds the specified threshold number of queued requests. The threshold number of queued requests to IMail Anti-Virus Server is also configured. For more information, see “Specifying the threshold number of queued requests” on page 24.

---

### To specify an alert interval during installation or to change the alert interval in the configuration file:

- At `LoadExceededAlertInterval=`, replace the existing interval with the new interval.

## Specifying the threshold number of queued requests

When the number of scan requests to IMail Anti-Virus Server exceeds the number of scan threads available, incoming requests are queued until a thread becomes available. When the number of queued requests to IMail Anti-Virus Server exceeds the specified threshold number, IMail Anti-Virus Server is considered to be at maximum load. This threshold number of queued scan requests is configured during installation and can be changed by editing the configuration file. The default setting is 100.

---

### Note

IMail Anti-Virus Server continues to queue all incoming requests, even after the threshold is exceeded. You can set options to log periods of time when the anti-virus server is at maximum load and to generate Load Exceeded alerts at a prescribed interval.

---

### To change the threshold number of queued requests to IMail Anti-Virus Server in the configuration file:

- At LoadMaximumQueuedClients=, type the desired maximum number of queued requests.

### Specifying what to log

Standard logging for IMail Anti-Virus Server is divided into three categories of information to be logged: information, warnings, and errors. Editing the configuration file lets you enable entire categories or selectively enable specific types of log entries.

In the configuration file, the options for logging are listed as shown:

LOGAllErrorsEnable=
LOGAllWarningsEnable=
LOGAllInfoEnable=
LOGCrashAlertEnable=
LOGStartupAlertEnable=
LOGShutdownAlertEnable=
LOGDefUpdateAlertEnable=
LOGDefErrorAlertEnable=
LOGLoadExceededAlertEnable=
LOGInfectionAlertEnable=
LOGFileScanAlertEnable=
LOGSNMPSMTPAlertEnable=

The first three options in the configuration file are the LOGAll options. If you activate logging by category, enable only the LOGAll options you want.

For example, if you enable LOGAllErrorsEnable, the individual error messages that fall into that category are enabled and do not need to be enabled individually (as shown in the following table).

Category	Category definition	Specific log entries enabled
LOGAllErrorsEnable=	When enabled, all errors are logged	LOGCrashAlertEnable LOGDefErrorAlertEnable LOGLoadExceededAlertEnable LOGSNMPSMTPAlertEnable
LOGAllWarningsEnable=	When enabled, all warnings are logged	LOGInfectionAlertEnable
LOGAllInfoEnable=	When enabled, IMail Anti-Virus activity information is logged	LOGStartupAlertEnable

To enable only selected logging options, set only those options and do not enable the LOGAll entries.

Logging option	Definition
LOGCrashAlertEnable	Logs all instances of IMail Anti-Virus Server crashes
LOGStartupAlertEnable	Logs all instances of IMail Anti-Virus Server start-up
LOGShutdownAlertEnable	Logs all instances of IMail Anti-Virus Server shutdown
LOGDefUpdateAlertEnable	Logs all instances of IMail Anti-Virus Server virus definitions updates
LOGDefErrorAlertEnable	Logs all errors that occur in virus definitions updates
LOGLoadExceededAlertEnable	Logs all instances when maximum load is exceeded for IMail Anti-Virus Server
LOGInfectionAlertEnable	Logs all virus infections found in scanned files
LOGFileScanAlertEnable	Logs all files scanned Note: This logging option is Off by default even when all three LOGAll options are enabled. This option should be enabled only for debugging purposes. Activating this logging option for general logging degrades performance significantly.
LOGSNMPSMTPAlertEnable	Logs all errors in sending alerts that result in no alert being sent (neither the primary nor the secondary SMTP server was available)

**To change the IMail Anti-Virus Server settings for logging in the configuration file:**

- At each logging option shown in the configuration file, type **1** to activate that logging option or **0** to deactivate the option.

For more information, see “Viewing standard logs” on page 14.

## Activating SMTP alerting

SMTP alerting is available for IMail Anti-Virus Server. When you enable alerting you must provide the requested information for delivery of the alert messages. You can activate SMTP alerting and selectively enable specific alerts.

In the configuration file, the SMTP alerting options are listed:

SMTPPrimary=
SMTPSecondary=
SMTPCrashAlertEnable=
SMTPStartUpAlertEnable=
SMTPShutDownAlertEnable=
SMTPDefUpdateAlertEnable=
SMTPDefErrorAlertEnable=
SMTPLoadExceededAlertEnable=
SMTPRecipList=
SMTPDomain=

The first two entries in the configuration file identify a primary and secondary SMTP server for forwarding alert messages. The last two entries specify the e-mail addresses for recipients and the local domain for the Anti-Virus server. To activate SMTP alerting, these four fields must be filled in.

The remaining SMTP entries are the specific alerts that are selectively enabled.

Specific alert	Definition
SMTPCrashAlertEnable	Sends an SMTP alert for all instances of IMail Anti-Virus Server crashes
SMTPStartUpAlertEnable	Sends an SMTP alert for all instances of IMail Anti-Virus Server start-up
SMTPShutDownAlertEnable	Sends an SMTP alert for all instances of IMail Anti-Virus Server shutdown
SMTPDefUpdateAlertEnable	Sends an SMTP alert for all instances of IMail Anti-Virus Server virus definitions updates
SMTPDefErrorAlertEnable	Sends an SMTP alert for all errors that occur in virus definitions updates
SMTPLoadExceededAlertEnable	Sends SMTP alerts (at the configured alert interval) for periods of time when the maximum load is exceeded for IMail Anti-Virus Server

For more information on configuring the alert interval, see “Specifying the alert interval” on page 24.

**To activate SMTP alerting for IMail Anti-Virus Server in the configuration file:**

- 1 At SMTPPrimary=, type the IP address of the primary SMTP server that will forward alerts.
- 2 At SMTPSecondary=, type the IP address of a secondary SMTP server that will forward alerts if communication with the primary SMTP server fails.
- 3 At each specific alert option shown in the configuration file, type 1 to activate that alert or 0 to deactivate the alert.
- 4 At SMTPRecipList=, type the e-mail addresses for the recipients of SMTP alerts. Separate multiple addresses with a comma or space.
- 5 At SMTPDomain=, type the local domain for IMail Anti-Virus Server.

The domain name is added to the **From** field for SMTP alert messages, so that SMTP alert messages generated by IMail Anti-Virus Server originate from  
*ScanServer@<servername>.<domainname>*  
where <servername> is the name of the machine running IMail Anti-Virus Server and <domainname> is the SMTP Domain supplied here.

For more information, see “Customizing alert messages” on page 14.

**Specifying which file types to scan**

Viruses are found only in file types that contain executable code. Since it is not necessary to scan every file type, bandwidth and time can be saved by limiting the files to be scanned to only those file types that can contain viruses. IMail Anti-Virus Server is configured by default to scan only certain file types based on file extension. By editing the configuration file, you can configure IMail Anti-Virus Server to scan all file types regardless of extension, or you can edit the default list of extensions.

The ExtensionList setting in the IMail Anti-Virus Server configuration file is preconfigured to contain the file extensions

recommended for virus scanning. Extensions in the list are specified with a period and are separated by a semicolon (for example, “.com;.doc;.bat;.foo”). To specify scanning of files with no extension, use two adjacent semicolons (for example, “.com;.exe;;”). To configure IMail Anti-Virus Server to scan all files regardless of extension, comment out the ExtensionList line in the configuration file. (If the extension list is missing from the configuration file or if the list is blank, all files are scanned by IMail Anti-Virus Server.)

---

#### **Note**

Comment out the ExtensionList line rather than delete the ExtensionList so that you retain the default list of extensions for future use.

---

#### **To edit the extension list:**

- At ExtensionList=, add or delete the extensions you want.

**To comment out the ExtensionList line in the configuration file so that IMail Anti-Virus Server scans all file types regardless of extension:**

- At the beginning of the ExtensionList= line, type a #.

