Sybari®
A Microsoft® Subsidiary

Antigen
for Instant Messaging

Antigen for Instant Messaging Quick Start Guide

Published: December 2005

LEGAL NOTICES

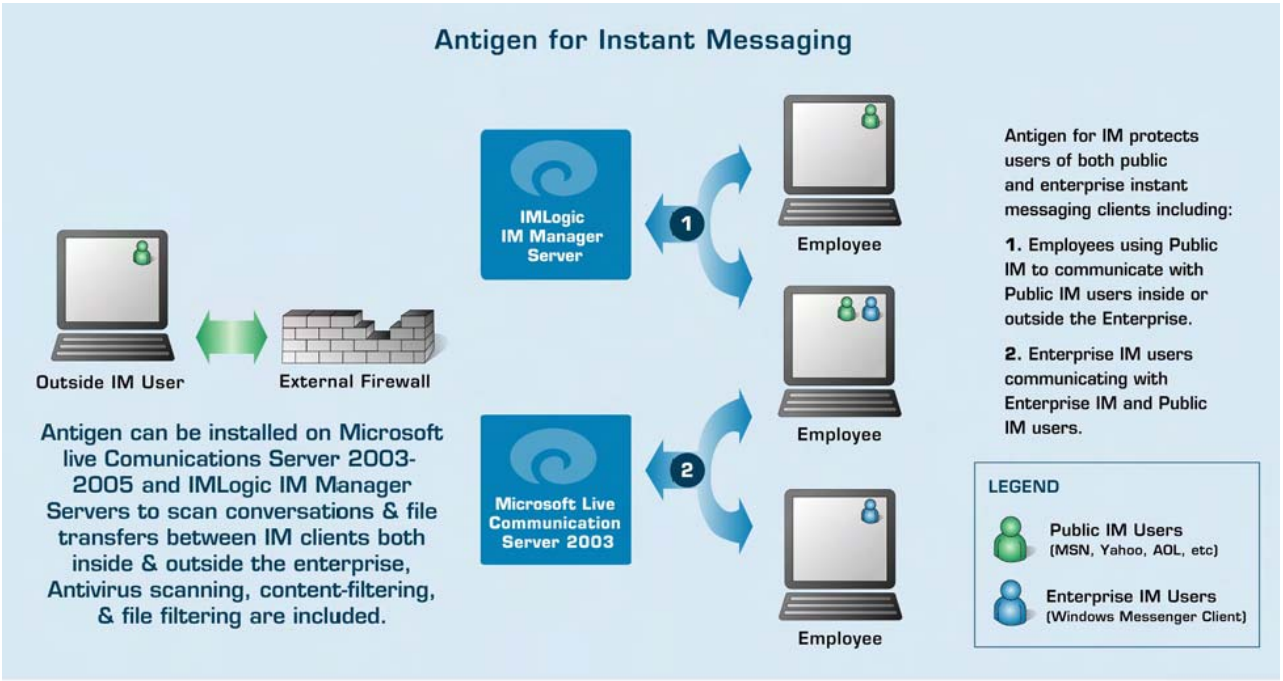
Contents

Chapter 1 - Introduction

Introducing Antigen for IM

Congratulations on selecting Antigen for Instant Messaging, a reliable, high-performance anti-virus and document filtering solution for Microsoft's Live Communications Server and IMLogic's IM Manager. This Quick Start Guide will help you install and configure Antigen for IM as quickly and simply as possible so that you can begin protecting your resources. Please note, however, that this guide is not intended to replace Antigen for IM's comprehensive documentation, nor is it meant to provide a collection of best practices.

Here is a pictorial representation of how Antigen for IM works:



Components

Antigen Service
Acts as the configuration and monitoring agent on the server to which the Sybari Client connects.

Antigen Administrator
Used by the administrator to configure and run Antigen locally or remotely.

Antigen Central Manager
Installs, upgrades, and uninstalls Antigen for IM on multiple servers.

Antigen Quarantine Manager
Provides Administrators a way to analyze and manage the information contained in the Quarantine database on one or more IM servers.

Licensing

Antigen for IM uses a license file to enable product subscriptions. Antigen for IM ships with a basic set of scan engines, and you can purchase additional ones as needed. To upgrade your evaluation copy of Antigen for IM to a full licensed version, you must obtain a license file (license.cfg) from Sales and install it. The license file also controls access to the antivirus engines and unlimited updates of virus signature files. For more information on licenses, see the "Installation" chapter.

Chapter 2 - Installation

Installing Antigen for IM is a simple process, providing protection for your IM communications in minutes. Antigen for IM supports local and remote installations on both Microsoft Live Communications Server 2003/2005 and IMLogic IM Manager.

Antigen for IM requires that MDAC (at least version 2.7) and Jet 4.0 SP3 be installed on IM servers (both are included in Windows 2003). If they are not present, Antigen for IM will provide the option of installing them prior to the Antigen for IM install (see below for more information).

Please Note: Antigen for IM setup wizards can be used to install the product to a local IM server, to a remote IM server, or to a local workstation, as a "Client Only" installation.

To begin the installation procedure, run SETUP.EXE from the directory containing the Antigen for IM installation files. The installation wizard will guide you through the install.

System Requirements

These are the minimum requirements necessary to install Antigen for IM on a server and on a workstation. Administrators must have Domain rights and Local admin rights to install Antigen for IM on either LCS or IM Manager servers.

Minimum Server Requirements

- Windows 2003
- Microsoft Live Communications Server 2003 or 2005, or IMLogic IM Manager
- SMTP Server (for SMTP notifications)
- 64 MB of Available Memory
- 100 MB of Available Disk Space
- Intel Processor

Minimum Workstation Requirements

- Windows NT Workstation 4.0 or Windows 2000 Professional
- 10 MB of Available Memory
- 10 MB of Available Disk Space
- Intel Processor

Installing On a Local Server

To install Antigen for IM on a local IM Server, log in to the local machine using an account that has administrator rights.

Follow the initial setup panels until you are prompted by the “Installation Location” panel. To install on a local server, choose “Local Installation”. These are the installation steps.

1. If MDAC or Jet is not installed, Antigen for IM will ask if you would like the component installed on the server. Follow the on-screen instructions to complete the installation. After MDAC or Jet has been installed, you will have to run SETUP.EXE again, in order to install Antigen for IM.
2. Choose “Server - Admin console and scanner components”.
3. Indicate if you want to install Antigen Central Manager and Antigen Quarantine Manager. The ACM provides centralized control of many Antigen for IM management tasks when you create and distribute “jobs” to other servers. If you are installing Antigen for IM on a single server, there is no need to install the ACM. For more information about the ACM, see the “Antigen Central Manager” chapter in the Antigen for IM *User Guide* and see the Configuring Jobs section of the “Configuring Antigen” chapter in this guide. The Antigen Quarantine Manager makes it simple to view and manage items in quarantine. However, if you will have few quarantined items, you can view them through the normal Sybari Client. For more information about the AQM, see the “Reporting and Statistics” chapter in the Antigen for IM *User Guide*.
4. You will be prompted to select which IM software you are running on the server: Select Microsoft Live Communications Server or IMLogic IM Manager.
5. At this point, setup will verify that the IM Server is installed and running.
6. Choose the Destination Directory. **Default:** Program Files\Sybari Software\Antigen for IM.
7. Choose the Start Menu Program Folder. **Default:** Antigen for IM.
8. If you would like Antigen for IM to send SMTP notifications to the IM Administrator, enter information about your SMTP server. You will need the server name or IP address, as well as a Username and Password, if necessary for your environment.
9. **LCS Installs Only:** Create the account that Antigen for IM will use to send IM notifications to senders and recipients when a virus is found or a message is filtered. For more information about creating an Antigen IM user account prior to installation, see the Creating An “Antigen IM” User Account section in the “Configuring Antigen” chapter.
10. Review the Install Settings and accept or correct as needed.
11. Antigen for IM will install all the required files.
12. Antigen for IM will start the IM services.
13. View the ReadMe.

Installing On Pooled LCS 2005 Servers

Antigen for IM can be installed on Pooled LCS servers. It is *important*, however, to configure Antigen for IM identically on each server to ensure that it runs and scans properly. We recommend that Administrators configure Antigen for IM on one server and then use the Antigen Central Manager (ACM) to push out configuration templates to the other servers in the Pool, thereby ensuring that all servers are configured identically. For more information on using templates, see the "Templates" chapter in the Antigen for IM *User Guide*.

Installing On a Remote Server

To install Antigen for IM on a remote IM Server, you will need to log into your local machine using an account that has administrator rights to the remote machine.

To install Antigen for IM on a remote IM Server, follow these steps:

1. Follow the initial setup panels until you are prompted by the "Installation Location" panel. Choose "Remote Installation / Uninstallation".
2. Enter the following information:

   Server Name: The name of the machine to which you are installing Antigen for IM.

   Share Directory: The temporary location that the remote install will use while setting up Antigen for IM. The default is C$.
3. If MDAC or Jet is not present on the remote server, Antigen for IM will ask if you would like the component installed. Once initiated, the MDAC or Jet installation will proceed in silent mode.

   Please Note: If a reboot is required after MDAC or Jet is installed, Antigen for IM will restart the server automatically and then continue installing Antigen for IM on the remote server.
4. Indicate if you want to install Antigen Central Manager and Antigen Quarantine Manager. The ACM provides centralized control of many Antigen for IM management tasks when you create and distribute "jobs" to other servers. If you are installing Antigen for IM on a single server, it is not necessary to install the ACM. For more information about the ACM, see the "Antigen Central Manager" chapter in the Antigen for IM *User Guide* and see the Configuring Jobs section of the "Configuring Antigen" chapter in this guide. The Antigen Quarantine Manager makes it simple to view and manage items in quarantine. However, if you will have few quarantined items, you can view them through the normal Sybari Client. For more information about the AQM, see the "Reporting and Statistics" chapter in the Antigen for IM *User Guide*.
5. You will be prompted to select which IM software you are running on the server: Select Microsoft Live Communications Server or IMLogic IM Manager.
6. At this point, setup will verify that the IM Server is installed and running.

7. Select “Update on Install” to have all of your licensed engines brought up to date before being placed online. If you do not want Antigen for IM to update the antivirus scan engines after install, clear “Update on Install”.
8. Choose the Destination Directory. **Default:** Program Files\Sybari Software\Antigen for IM.
9. Choose the Start Menu Program Folder. **Default:** Antigen for IM.
10. If you would like Antigen for IM to send SMTP notifications to the IM Administrator, enter information about your SMTP server. You will need the server name or IP address, as well as a Username and Password, if necessary for your environment.
11. **LCS Installs Only:** Create the account that Antigen for IM will use to send IM notifications to senders and recipients when a virus is found or a message is filtered. For more information about creating an Antigen IM user account prior to installation, see the Creating An “Antigen IM” User Account section in the “Configuring Antigen” chapter.
12. Review the install settings and accept or correct as needed.
13. Antigen for IM will install all the required files.
14. Antigen for IM will start the IM services.
15. View the ReadMe file.

Please Note: Upon installation, Antigen for Im is configured to allow everyone with administrative rights to the server access to AntigenService. To restrict access to AntigenService, you can use DCOMCNFG to modify the security settings. For more information about securing access to AntigenService, see Securing The Service in the “Configuring Antigen” chapter.

Installing To Multiple Servers

The Antigen Central Manager (ACM) utility installs, upgrades, and uninstalls Antigen for IM on multiple servers. The ACM can be run by clicking on Antigen Central Manager in the Start menu. For directions on using the ACM to install Antigen for IM to Multiple Servers, see Antigen Central Manager in the “Sybari Client” chapter of the Antigen for IM *User Guide*.

Installing On a Client Only

Performing a Client-Only installation will install the Sybari Client onto any Windows Workstation or Server that can then be used to centrally manage the Antigen Service running on remote IM Servers. Client-Only installation requires approximately 2.5 MB of disk space.

1. Follow the initial setup panels until you are prompted by the “Installation Location” panel. At that point, choose “Local Installation”.
2. Choose “Client - Admin Console Only”.
3. Choose the installation directory. **Default**: Program Files\Sybari Software\Antigen for IM.
4. Choose the Start Menu Program Folder. **Default**: Antigen for IM.

Installing the License File

The license file can be installed and activated in any of three ways:

1. Prior to installation, replace the license.cfg file found in the Antigen install folder with the one you downloaded from Sybari's website. You should rename and keep the original license.cfg file in the event that you need to roll back to it. Once the new license.cfg file has been added to the Install Folder you may install Antigen for IM normally.
2. After installation, you can run the ACM job "Deploy License" as described in the "Sybari Client" chapter of the Antigen for IM *User Guide*.
3. After installation, you can manually add the file to the Antigen install folder, navigate to that folder, and run the AntigenStarter from the command line with the "l" option (that is, the letter "L"):

```
antigenstarter l
```

Upgrading

The Antigen for IM install detects previous installations of Antigen for IM. Local and remote installs provide the option of uninstalling the previous version or upgrading it. Upgrading an installation only requires that you provide the password for the User Account that the Antigen Services run under (for security reasons, Antigen for IM does not store this). Antigen for IM retains all of your previous settings. Upon upgrading, additional features may be added to the product, based on your environment.

When upgrading Antigen for IM, all scan jobs will have their template settings configured to "none", in order to prevent users from inadvertently overwriting existing settings. To deploy templates, you will need to change this setting on each server to "default" or to a named template. For more information on configuring scan job template settings, see the "Templates" chapter of the Antigen for IM *User Guide*.

Evaluation Version

Sybari provides a fully-functional version of Antigen for IM for a 30-day evaluation. After 30 days, Antigen for IM will continue to operate and report detected file attachments, but it will cease to clean them.

Chapter 3 – Configuring Antigen

Before you use Antigen for IM for the first time, there are some steps that should be performed. For more detailed information on these procedures, see the Antigen for IM *User Guide*.

Creating an "Antigen IM" User Account

You will need to create an "Antigen IM" user account for notifications (**LCS installs only**). This account will be used by Antigen for IM to send notifications to users and administrators about virus and filter events. To create the account, follow these steps:

1. Create a domain account for Antigen Notifications. For example: "AntigenIM".
2. Add the AntigenIM user to the local Administrators group on the LCS Server.
3. Add the AntigenIM user to the local RTC Server Applications group on the LCS Server.
4. Modify the properties of the AntigenIM user and enable Live Communications. Fill in the required information.

Securing the Service

AntigenService runs on the IM Server and controls all the back-end functionality of Antigen. It services requests from the Sybari Client, controls the scanning processes, generates e-mail notifications, and stores virus incident data to disk. (This data can then be viewed using the Sybari Client.) AntigenService is not installed in a "Client-Only" installation.

The AntigenService utilizes Distributed COM (DCOM) to launch and authenticate Sybari Client connections. You can create an access list of authorized Windows users who can connect to the AntigenService utilizing the Sybari Client.

To edit the default settings for the AntigenService, follow these steps:

1. Open a command window.
2. Enter DCOMCNFG. The Component Services dialog appears.
3. Choose "AntigenService" from the Applications list.
4. Right-click, and then select **Properties**.

Once the identity of a user account has been configured you can use the Access Lists in the **Security** tab of the Properties dialog to control who has rights to access the AntigenService, launch the AntigenService, or change the DCOM configuration. To learn more about Service, see the "Antigen Services" chapter of the Antigen for IM *User Guide*.

Relocating Data Files

Antigen for IM stores program settings, as well as scanning activity information (including the Quarantine Area), on the file system. If you wish, you may relocate the database files at any time after installation. For more information on relocating the databases, see the Moving The Databases section in the "Reporting and Statistics" chapter of the Antigen for IM *User Guide*.

The Sybari Client

The Sybari Client is used by an administrator to configure and run Antigen for IM locally or remotely. For the Sybari Client to launch successfully, the "AntigenService" and the IM server must be running on the machine to which the Sybari Client is connecting. Since the Sybari Client is the front end of the Antigen for IM software, it can be launched and closed without affecting the back end processes that are being performed by the Antigen Services. The Sybari Client may also be run in a "Read-Only" mode to provide access to users who do not have permission to change settings or run jobs, but who may need to view information provided through the UI.

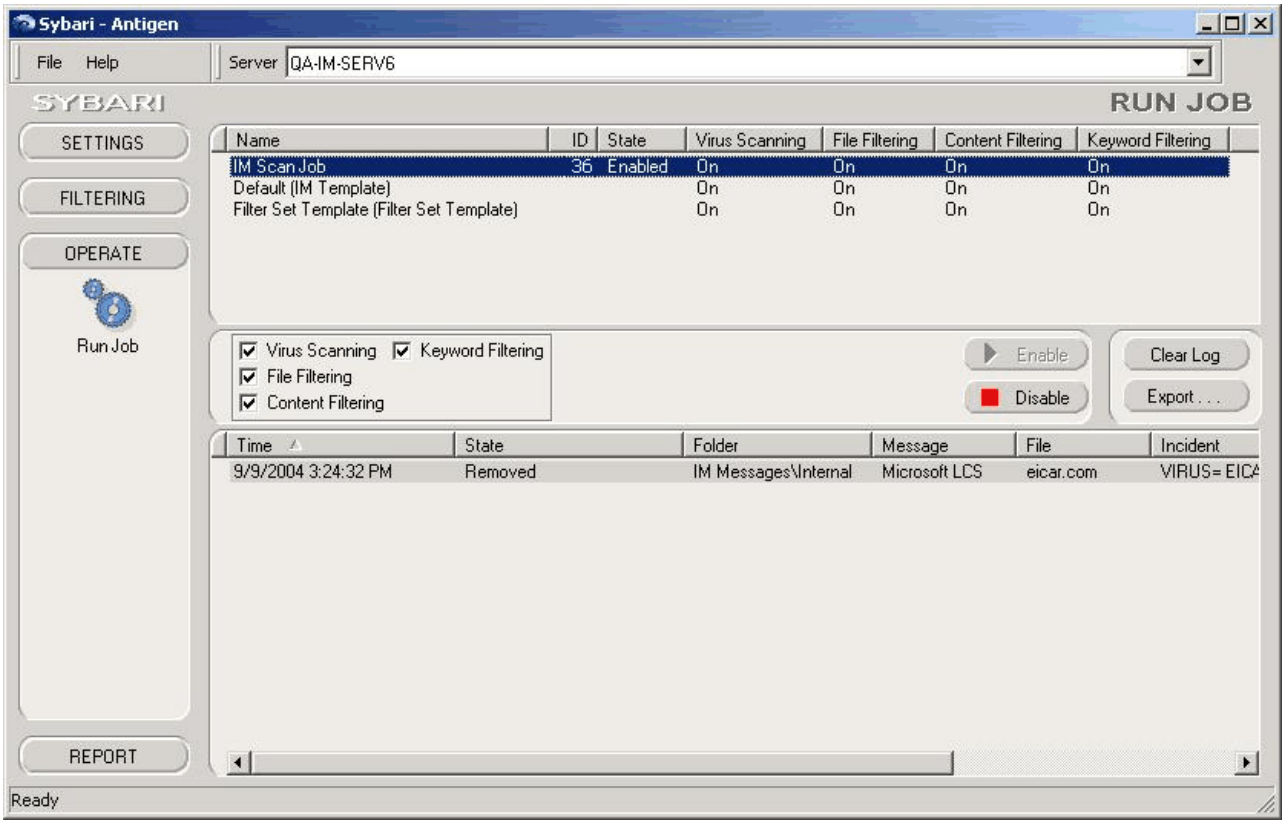
To run the Sybari Client, select it in Start/Programs/Antigen for IM.

Connecting To a Local Server

The first time the Sybari Client is launched, it will prompt you to connect to the IM Server running on the local machine. You can use the server name or "local" alias to connect to the local IM server.

Sybari Client Overview

The Sybari Client UI contains the Shuttle Navigator on the left and the Work Panels on the right, as shown below:



There are four shuttles in the Shuttle Navigator:

SETTINGS Lets you access the work panels to configure Scan Jobs, Anti-Virus, Scanner Updates, Templates, and General Options.

FILTERING Lets you access the work panels to configure File Filtering, Keyword Filtering, Content Filtering, Whitelist Filtering, and Filter Lists.

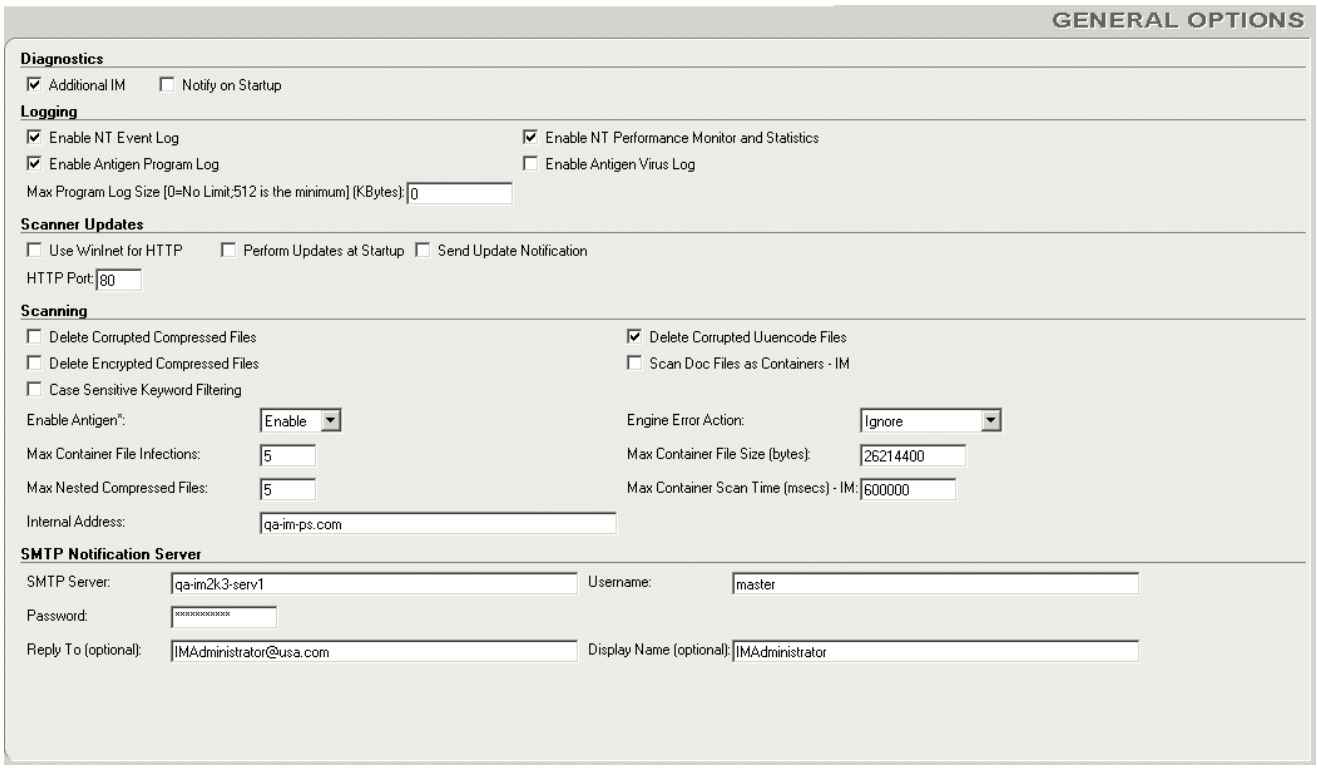
OPERATE Lets you access the work panels to run anti-virus jobs.

REPORT Lets you access the work panels for Notification Configuration, the Incidents View, and the Quarantine area.

All of the shuttle navigators and their uses are discussed in the Antigen for IM *User Guide*.

General Options

General Options, accessed from the SETTINGS shuttle of the Sybari Client, provides access to a variety of system-level settings for Antigen for IM, eliminating the need to directly access the Registry in order to change them.



While there are many options that can be controlled through the General Options panel, each of them has a default (enabled/disabled or a value), which is probably the correct one for your enterprise; it is rare that any of these settings would need to be changed. However, several of the settings were entered during installation and you might need to change one of them from time to time. You can find a list of the General Options and their definitions in the "Sybari Client" chapter of the Antigen for IM *User Guide*.

Configuring File Scanner Updating

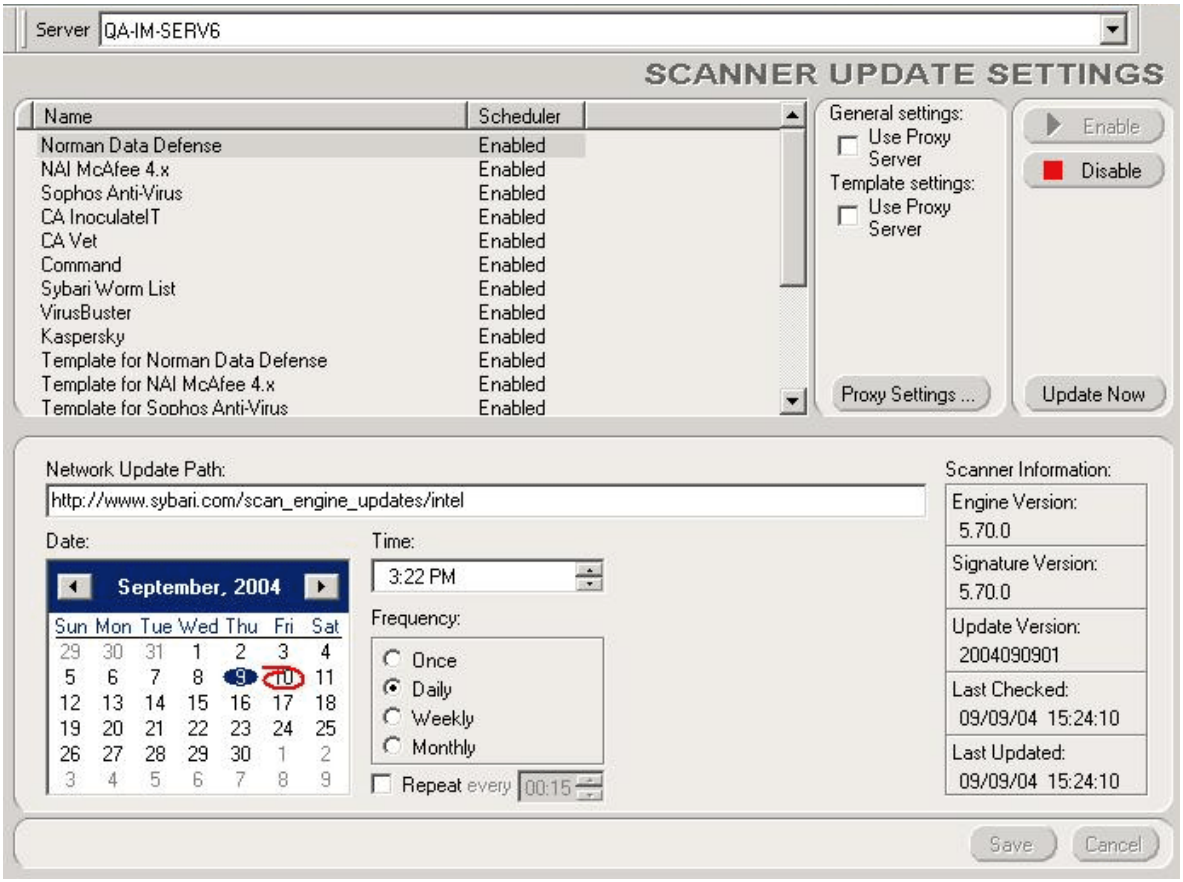
The standard Antigen for IM license includes four antivirus engines: one each from Norman and Sophos, and two from Computer Associates (InoculateIT and Vet). When additional engines are purchased, they are activated the first time you run an engine update. After installing Antigen for IM, all of your licensed engines are immediately available.

Scan engine signature files and Sybari Worm List updates can be downloaded automatically from the Sybari FTP Server, the Sybari HTTP Server, or another IM Server running Antigen for IM from a UNC share. Using the Sybari Client to set a schedule for checking the FTP, HTTP, or IM Server for a new scan engine enables enterprises to be automatically protected against new viruses without

having to check versions or manually update the files. Once Antigen for IM has automatically downloaded an updated scan engine, all subsequent mail is scanned with the new signature files. For more information on updating scanners, see the “File Scanner Updating” chapter of the Antigen for IM *User Guide*.

Scanner Update Settings

To set the schedule times for updating the scanning engine, select SETTINGS in the Shuttle Navigator, and then choose **Scanner Updates**. The Scanner Update Settings dialog appears:



The top portion shows a list of supported file scanners and the Sybari Worm List. The bottom portion contains the updating schedule for the highlighted scanner, along with information on that scanner.

Scheduling an Update

In the engine list, highlight the scan engine for which you will be downloading updates.

Network Update Path

You can enter any of these paths in this field:

- To get updates directly from Sybari's FTP server, enter:

  ftp://ftp.sybari.com/scan_engine_updates/intel
- To get updates directly from Sybari's HTTP server, enter:

  http://www.sybari.com/scan_engine_updates/intel
- To reference another IM Server that has the update you need, specify the UNC path to that server. (For more information about sharing updates, see Distributing Updates in the "File Scanner Updating" chapter of the Antigen for IM *User Guide*.)

To restore the default Sybari server path, right click in the **Network Update Path** field and select either Default FTP Path or Default HTTP Path.

Date

Use the calendar to specify when to check for updates. Click the left and right arrows to control the month. Click a particular day to select it (it will turn blue).

Time

Set a time for the update to take place. Each of the three subfields (hour, minute, and AM/PM) can be selected and set separately. You can enter a time or use the up/down controls to change the current value.

Frequency

Select a frequency for the update. We recommend that you select Daily, and then set a Repeat interval to update multiple times during the day.

Repeat

Enable the Repeat function by selecting the checkbox and choosing a time interval (the minimum time is 15 minutes). We recommend that you check for updates *at least* every two hours. If a new engine is not available when the schedule runs, no updating is done for that engine.

Enabling Updates For an Engine

Use the **Enable** and **Disable** buttons to control whether the update check will be performed on a selected engine. All engine updates are *enabled* by default.

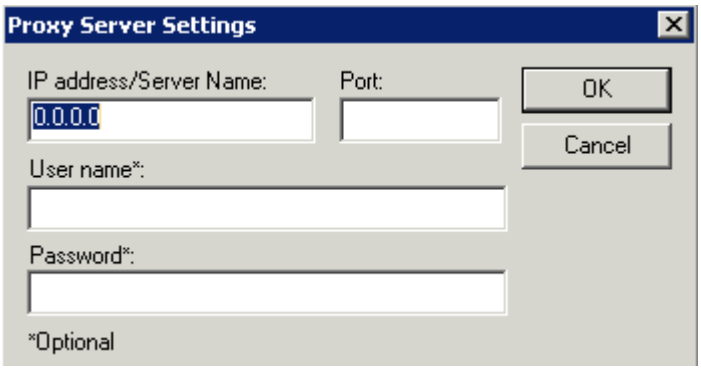
Scheduling Updates On Multiple Servers

When scheduling engine updates on multiple servers in an organization, we recommend staggering the updates by at least five minutes to prevent servers from timing out during the update process. Consider scheduling updates at off-hours (such as between midnight and 6:00 AM). You should also avoid scheduling updates on the hour or half-hour.

Updating Through a Proxy

In environments where the IM server(s) must access the internet through a proxy server, Antigen for IM can be configured to retrieve engine updates through that proxy.

There is a proxy section on the top of the Scanner Update Settings dialog. You can separately select to use a proxy server for General Settings and Template Settings. The **Proxy Settings** button opens the Proxy Server Settings dialog, in which you enter the attributes of the proxy server:



- **IP Address/Server Name -** The IP address or Server Name of the proxy server.
- **Port -** The Port number Antigen for IM should use.
- **User name -** The name of a user with access rights to the proxy server, if necessary.
- **Password -** The appropriate password for that user.

Once the proxy server settings have been entered, they are saved in both the filescanners.adb and template.adb files.

Deploying The Proxy Server Settings

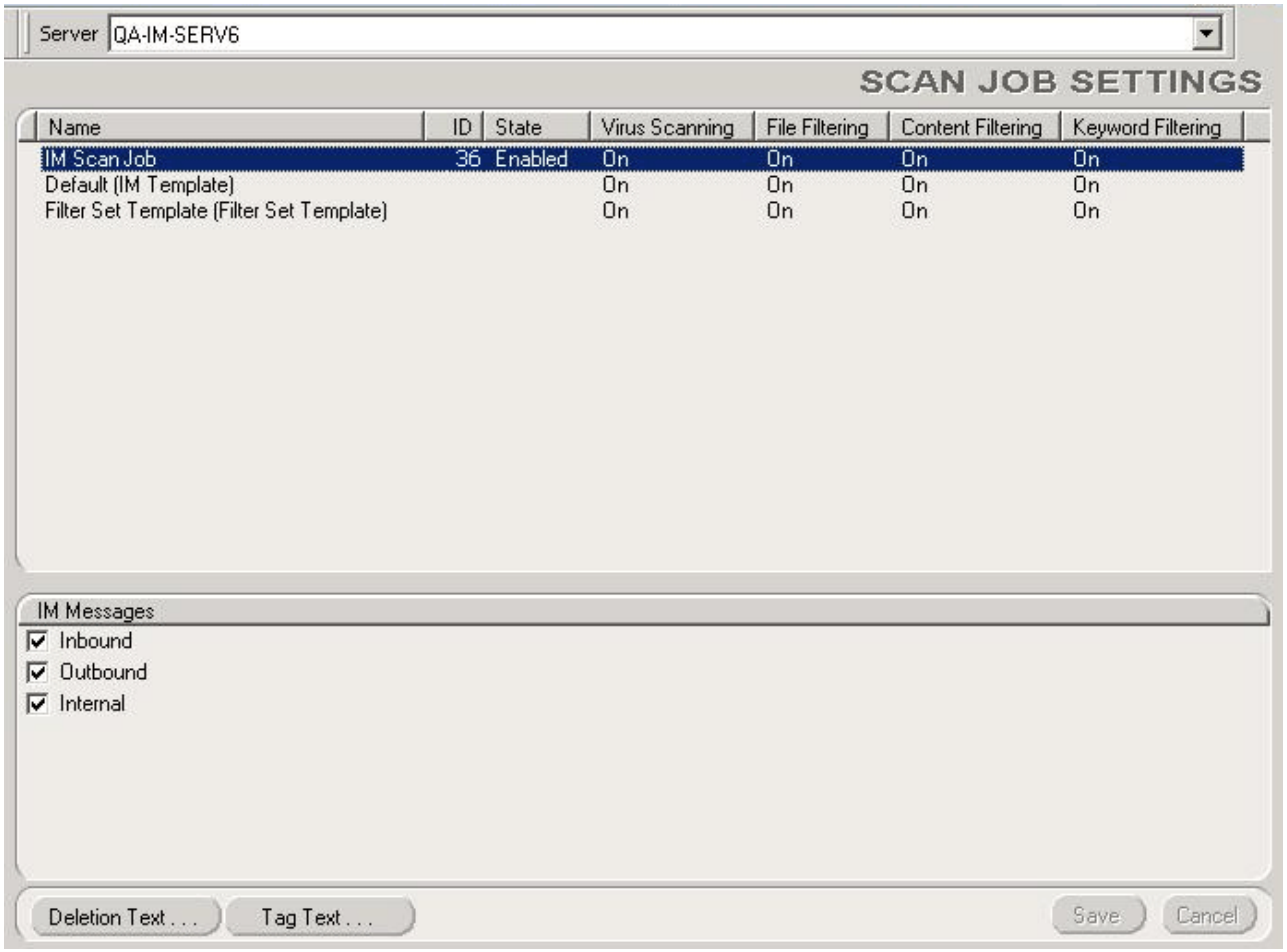
If you would like your local server to use the proxy server settings, select the **Use Proxy Server** checkbox in the General Settings section of the Scanner Update Settings screen. This causes Antigen for IM to use the configured proxy server for all engine updates.

If you would like to deploy the proxy server settings using the template.adb file, you must *also* select **Use Proxy Server** under Template Settings. If both are not selected, the proxy server settings will not deploy properly when the template.adb file is deployed to remote servers. For more information on templates, see the “Templates” chapter of the Antigen for IM *User Guide*.

Configuring the IM Scan Job

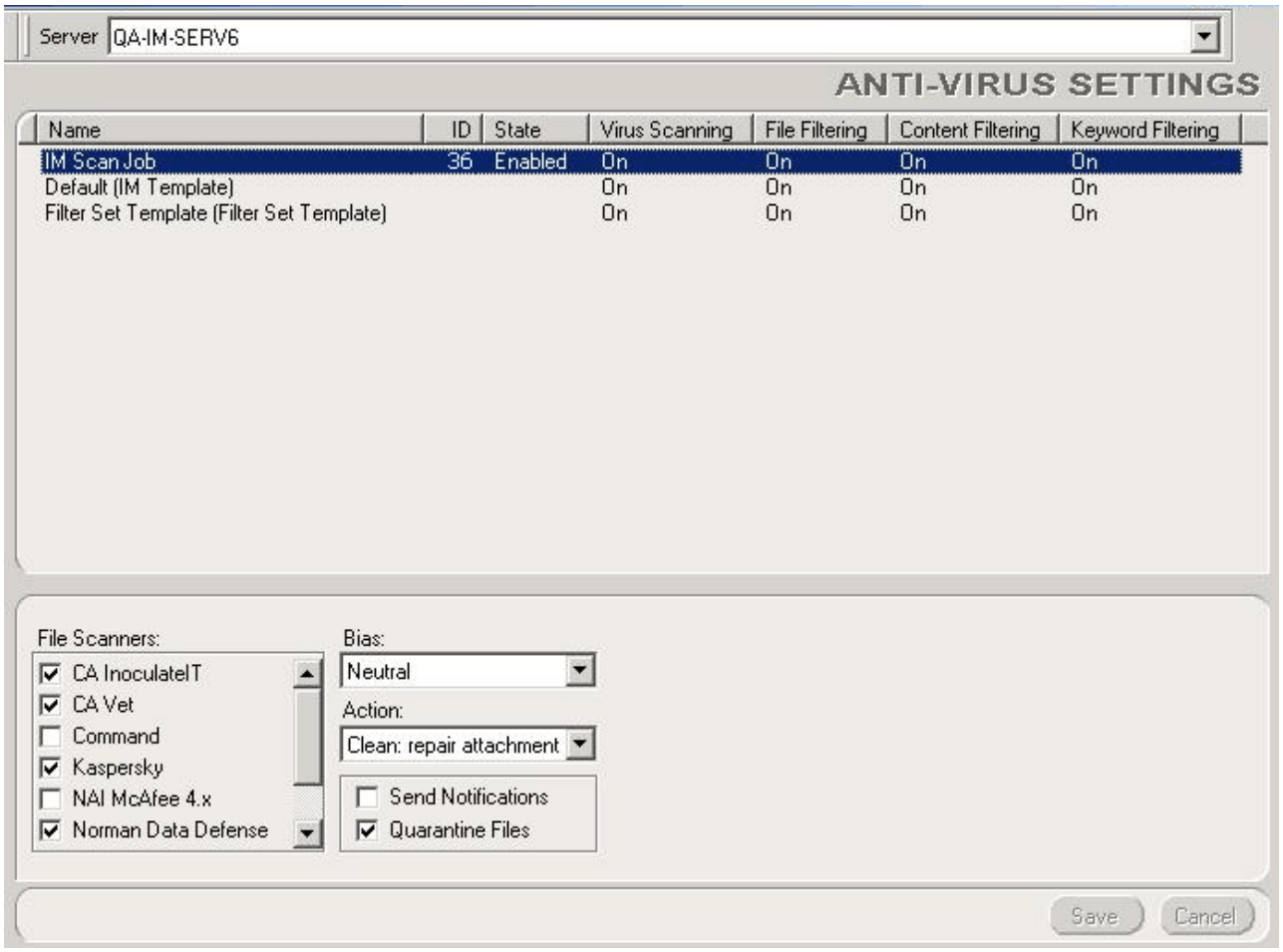
The IM Scan Job scans all IM messages relayed by the protected Antigen for IM servers for viruses and filter matches. To configure the IM Scan Job, follow these steps:

1. Select **Scan Job** from the SETTINGS shuttle. The Scan Job Settings dialog appears:



2. Highlight the IM Scan Job in the list of scan jobs.
3. In the bottom section of the UI, specify the message queues to be scanned: inbound, outbound, and/or internal. See Queues To Be Scanned, below.
4. Click the appropriate button to customize the Deletion Text (inserted when the contents of an infected file are deleted) and Tag Text (inserted when a message is “tagged” by Antigen for IM because it has been blocked), if desired (see Deletion Text and Tag Text, below).

5. Select Anti-Virus from the SETTINGS shuttle. The Anti-Virus Settings dialog appears:



6. Highlight the IM Scan Job.
7. Select the desired scan engines from the list in the File Scanners section of the UI.
8. Select a **Bias** value of Neutral. For more information about Bias, see the "Multiple Scan Engines" chapter of the Antigen for IM *User Guide*.
9. Select an **Action** of Clean. Antigen for IM will block any attachments that cannot be cleaned. For more information about Actions, see the "IM Scan Job" chapter of the Antigen for IM *User Guide*.
10. Select **Send Notifications**.
11. Select **Quarantine Files**.
12. Run the Scan Job. See the "Running the Scan Job" chapter.

Queues To Be Scanned

Antigen for IM offers flexibility in choosing which message queues to scan with the IM Scan Job. You can configure Antigen for IM (on the Scan Job Settings screen) to scan only the desired queues.

Scanning the Inbound Queue
Selecting Inbound configures Antigen for IM to scan all IM messages entering the domain. Messages are designated as Inbound if the message originated from, or was relayed through, an external server.

Scanning the Outbound Queue
Selecting Outbound configures Antigen for IM to scan all outgoing IM messages that leave your domain. Messages are designated as Outbound if at least one recipient has an external address.

Internal Scanning
Selecting Internal configures Antigen for IM to scan all mail that is being routed from one location to another, both inside your domain. Messages are designated as Internal if they originate from inside your domain and *all* the recipients are located inside your domain.

Deletion Text

Clicking **Deletion Text** (on the Scan Job Settings screen) displays a text field with the text used by Antigen for IM when replacing the contents of an infected file during a delete operation. You can place a custom message inside the deleted file attachments by modifying this text field.

Keyword Substitution Macros Used In Deletion Text

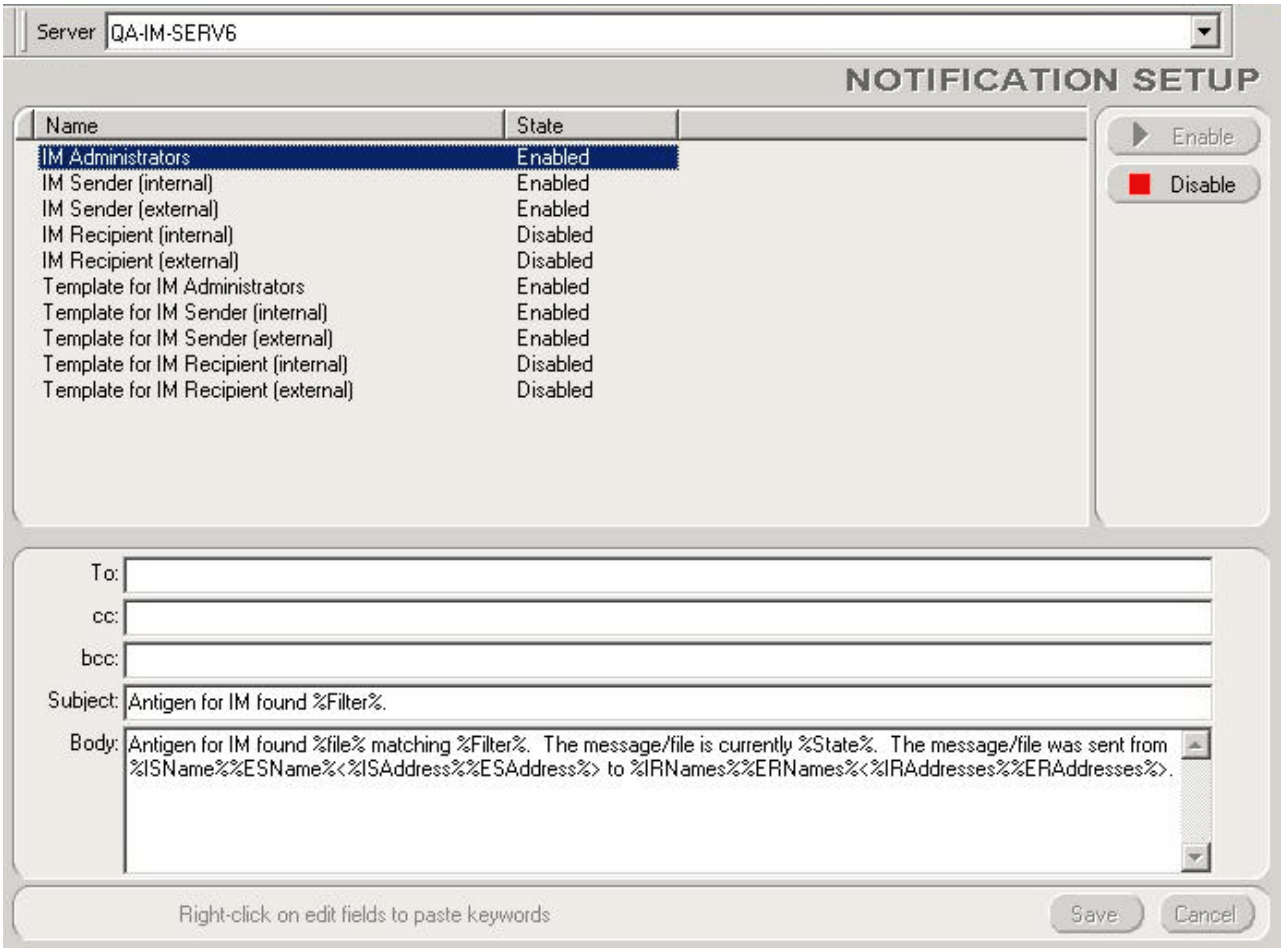
Antigen provides Keywords that can be used in the deletion text field to obtain information from the message in which the infection was found. For a list of available Keywords, see the “Keyword Substitution Macros” appendix in the Antigen for IM *User Guide*.

Tag Text

Clicking **Tag Text** (on the Scan Job Settings screen) displays a text field with the text used by Antigen for IM when a message matches a Content Filter and the action for the filter is set to “Identify: Tag Message”. (For more information about this Action, see the “Content Filtering” chapter in the Antigen for IM *User Guide*.) You can create a custom message by modifying this text field.

Configuring Notifications

There are numerous forms that allow administrators, senders (both internal and external), and recipients (both internal and external) to be notified of incidents. Each of these can be edited and customized by selecting **Notification** from the REPORT shuttle. The Notification Setup dialog appears:



Notification Roles

The top portion of the Notification Setup panel contains the list of default Notification “roles”. Each role can be enabled, disabled, and customized.

Antigen for IM can be configured to send different notifications to “internal” and “external” senders and recipients. To do so, select General Options from the SETTINGS shuttle and enter the domain names that should be sent internal notifications. Addresses should be entered as a semicolon-delimited list: for example: exampleone.com;exampletwo.net;examplethree.com. Any change to this value is immediately reflected in virus notifications. (For more information about General Options, see the “Sybari Client” chapter of the Antigen for IM *User Guide*.)

Default Notification Roles

IM Administrators - Alerts administrators of all viruses and filter matches detected on the server being protected by Antigen for IM. Typically, the notification is used for reporting the who, what, where, and when details of the infection, including the disposition of the virus, or filter match. These notifications would most likely use many keyword substitution macros For more on macros, see below and the "Keyword Substitution Macros" appendix of the Antigen for IM *User Guide*.

IM Sender (internal) - Alerts the sender of an infection or filter match, if that sender is an IM user in your organization.

IM Sender (external) - Alerts the sender of an infection or filter match, if that sender is an IM user outside of your organization.

IM Recipients (internal) - Alerts the recipient of an infection or filter match, if that recipient is an IM user in your organization.

IM Recipients (external) - Alerts the recipient of an infection or filter match, if that recipient is an IM user outside of your organization.

Template Categories - Each of the above categories also exists in the listing as a "Template for" item to aid you in deploying notification templates to remote servers. For more information on Templates, see the "Templates" chapter of the Antigen for IM *User Guide*.

Configuring Antigen For Internal Addresses

"Internal Addresses" must be identified in Antigen for IM so that the proper notifications can be sent to Senders and Recipients. For more information on configuring internal addresses, see General Options in the "Sybari Client" chapter of the Antigen for IM *User Guide*.

Enabling/Disabling a Notification

Immediately to the right of the list of the list of default Notification roles are buttons that allow you to enable or disable the selected Notification. The current status of each notification is displayed in the State column. Changes made to the status of each Notification take effect immediately.

Please Note: The Scan Job configuration controls the sending of any enabled notifications.

Configuring a Notification

The entries that you make in the lower portion of the Notification Setup dialog apply to the currently-selected Notification role. All changes take effect immediately upon saving them.

Recipients (To:, cc:, bcc:)
A semicolon-separated list of people and groups who will receive the notification. This list can include e-mail addresses, aliases, and groups.

Subject
The subject line text of the notification.

Body
The message that will be sent as the body of the notification. Administrators may also include the MIME headers in this field by inserting the %MIME% macro in the body field when configuring Notifications.

Keyword Substitution Macros

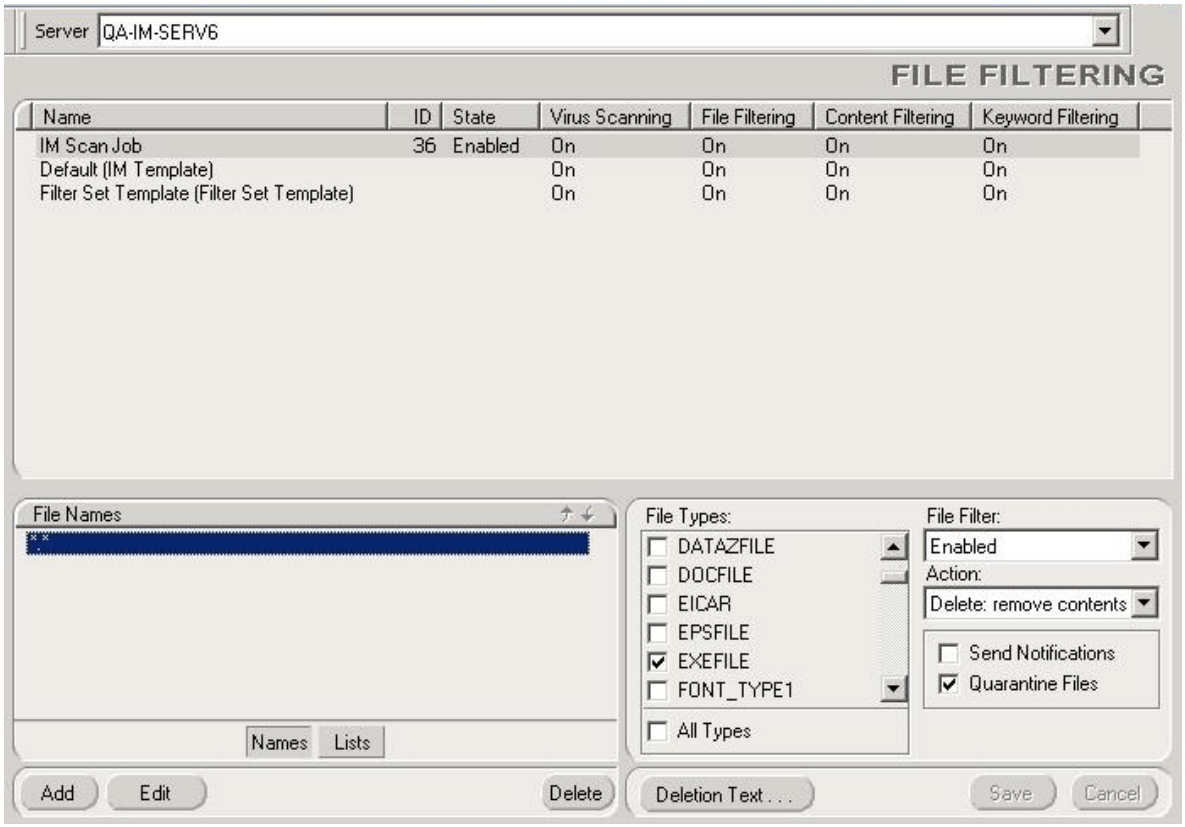
All fields can include **Keyword Substitution Macros** to obtain information from the message in which the infection was found or filtering was performed. For more on macros, see the "Keyword Substitution Macros" appendix of the Antigen for IM *User Guide*. For example, to include the name of the virus in the Subject line, you could use the %Virus% substitution macro, as follows:

> The %Virus% virus was found by Antigen for IM.

Configuring a File Filter

Antigen for IM's File Filter feature lets you search for attachments with a specific name, type, and/or size. Here's how to configure a file filter:

1. Select **File** from the FILTERING shuttle, and then click the File icon. The File Filtering dialog appears:



The top of the File Filtering dialog contains the list of configurable Scan Jobs. The bottom shows the configuration of the currently selected Scan Job.

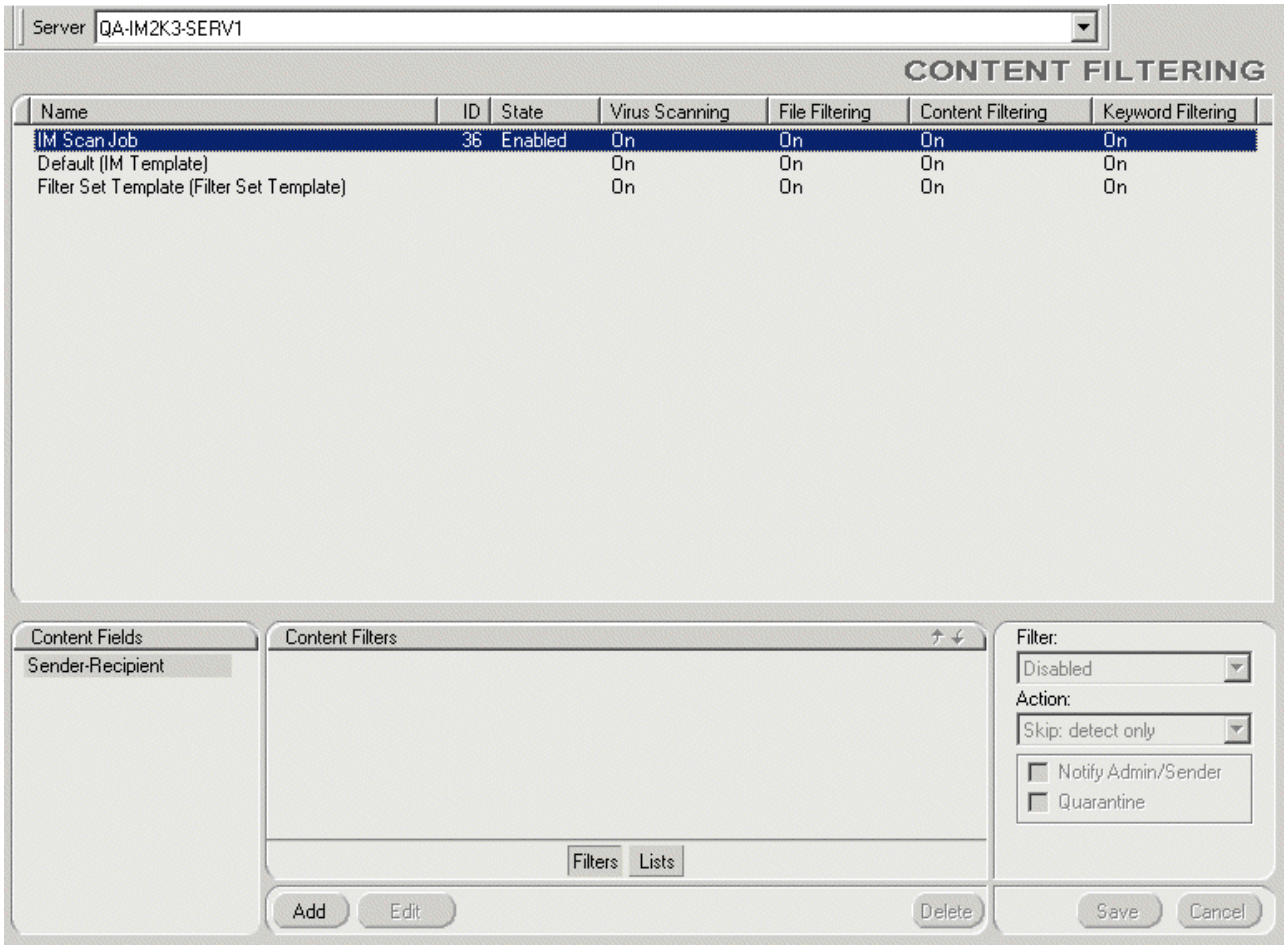
2. Select the IM Scan Job. You can then indicate specific files to detect, change the file types to be scanned, indicate the action to take, and whether to send notifications. When you have made your changes, click **Save**.
3. Click **Add** to enter the name of the filter, and then hit ENTER. For example, to prevent "resume.doc" from being sent or received, create a filter called "resume.doc". To make it more general, you could use an "*" wildcard: "resume.*" would filter any file whose name is resume, regardless of its extension. To learn more about other kinds of wildcards, see the "File Filtering" chapter of the Antigen for IM *User Guide*.
4. To only apply the filter to inbound messages, add the <in> prefix to the filter name (for example, "<in>resume.doc"). To only apply the filter to outbound messages, add the <out> prefix to the filter name (for example, "<out>resume.doc"). If there is no prefix, the filter is applied to inbound, outbound, and internal messages.
5. Select the appropriate File Type. The default is "All Types", but you can make the filter more efficient by selecting a single file type. If you know, for example, that you are searching for a Word Document, you can deselect All Types, and then select DOCFILE from the **File Types** list. If you're not quite sure of the type, you can add "resume.*" to the File Names List and leave the All Types check box selected. This will ensure that *all* files with the name "resume" will be detected, regardless of their extension or type.
6. Set the Action to **Block**.
7. Set the "File Filter" enabler to **Enabled**.
8. Select **Send Notifications** and **Quarantine File**.
9. Your new filter will now be used every time the IM Scan Job runs.

Please Note: You can avoid entering each file name individually by creating a Filter List in a text file and importing it into Antigen for IM. For more information about creating a Filter List, see Creating A New Filter List, below.

Configuring a Content Filter

Content Filtering allows you to filter messages based on sender/recipient/domain criteria. Here's how to configure a content filter:

1. Select **Content** from the FILTERING shuttle. The Content Filtering dialog appears:



2. Highlight the IM Scan Job.
3. Click **Add** to add a single sender/recipient name. Enter the sender or domain you would like to filter. To create a generic domain name filter, use the * (wildcard) character before the domain name. Wildcards can be used to enable such filters as "**@domain*.com" to filter all mail from a certain domain. Hit **ENTER**.
4. Set the Filter enabler to **Enabled**.
5. Choose an **Action** for the filter. The choices are "Purge" (deletes the message), "Skip: detect only" (records the number of files that meet the filter criteria, but allows the files to route normally), and "Identify: Tag" (replaces the original message with the "Tag Text", which is set on the Scan Job Settings dialog, reached by clicking **Scan Job** on the SETTINGS shuttle).
6. Indicate if notifications are to be sent and if the message is to be quarantined.
7. Click **Save** to save your new filter.

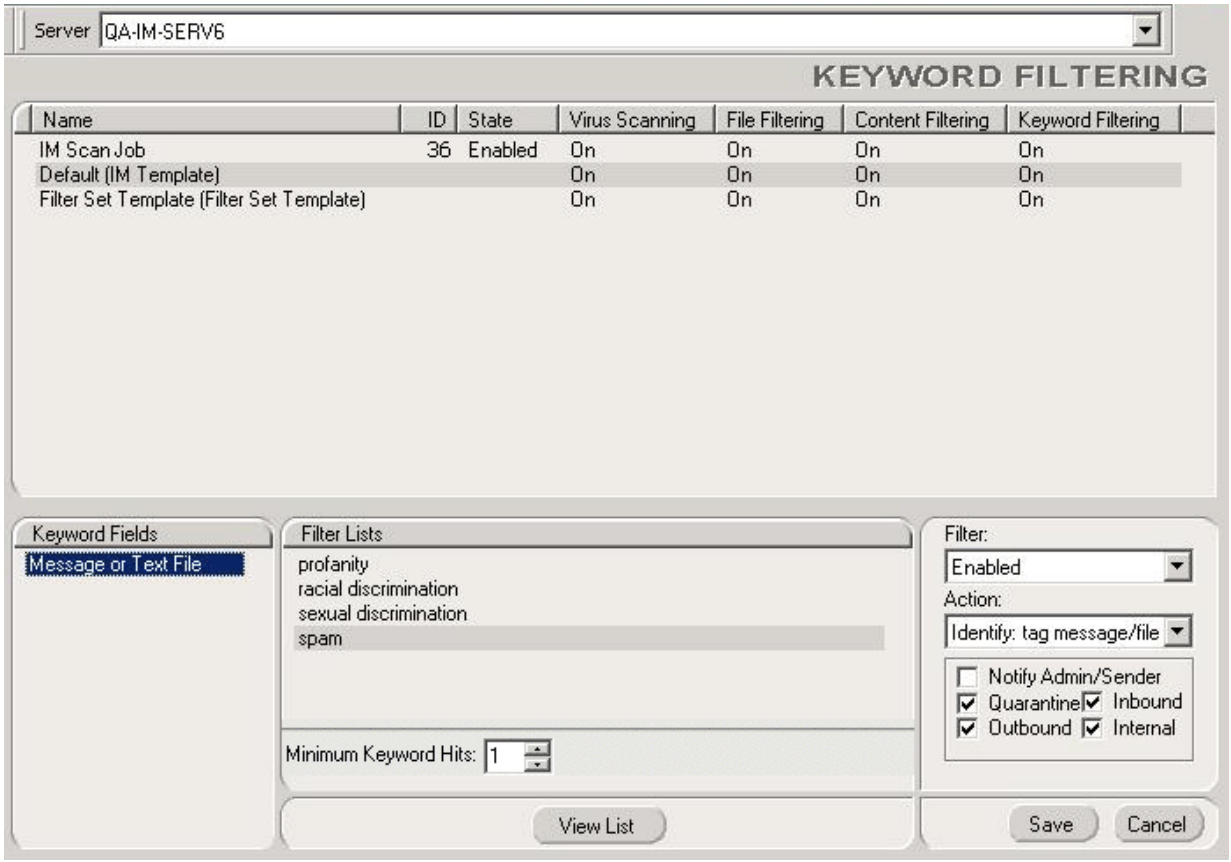
Please Note: You can avoid entering each sender/recipient name individually by creating a Filter List in a text file and importing it into Antigen for IM. For more information about creating a Filter List, see Creating a Filter List, below.

Enabling the Spam Filter List

The Spam Filter List is one of the default lists provided by Antigen for IM. (There are default filter lists for Profanity, Racial Discrimination, Sexual Discrimination, and Spam, although they are *disabled* by default.) Keyword Filtering identifies unwanted IM messages by analyzing the contents of the message body or text-based file attachments. By using keyword lists, you can filter messages and text attachments based on a variety of words, phrases, and sentences. You may modify these default lists, as needed, to suit the needs of your organization. (To create a filter list of your own, see Creating a Filter List, below.) Here's how to enable the Spam keyword filter.

Please Note: You are advised to customize the Spam Filter List to reduce false positives and increase detection. See Customizing the Spam Filter List, below.

1. Select **Keyword** in the FILTERING shuttle. The Keyword Filtering dialog appears:



2. Select the IM Scan Job.
3. Select the Spam filter list in the Filter Lists section.
4. Set the Filter enabler to **Enabled**.

5. Set the **Action** for Antigen for IM to take upon detecting a match to the filter criteria. The choices are: “Skip: detect only” (Records the number of files that meet the filter criteria, but allows the files to route normally), “Purge: eliminate message” (deletes the message), “Identify: tag message/file” (replaces the original message with the “Tag Text”, which is set on the Scan Job Settings dialog, reached by clicking **Scan Job** on the SETTINGS shuttle).
6. Indicate if you would like to send Notifications and/or Quarantine identified files.
7. Indicate which messages this filter applies to: Inbound, Outbound, or Internal.
8. Specify how many different keywords must be matched in order for the Action to be taken, by using the **Minimum Keyword Hits** field. The default is one (1).
9. Click **Save** to save your changes.

Customizing the Spam Filter List

In order to reduce false positives and increase detection, you should customize the default Spam Filter List. Here’s how:

1. Click **Filter Lists** in the FILTERING shuttle.
2. Select **Keywords** in the List Types section.
3. Select **Spam** in the List Names section.
4. Click **Edit/Import** to edit the list. The Edit Filter List dialog appears, displaying all the current items in the left-hand column.
   - To remove an item from the list, select it and click **Remove**.
   - To add an item to the list, click **Add**, type in the text, and then hit **ENTER**.
   - To import a list of items in an external text file, click **Import**, and then select the file.
5. Click **OK** when you are finished revising the list.
6. Click **Save** to save your changes.

Creating a New Filter List

In order to further customize filtering in Antigen for IM, here’s how to create your own filter lists:

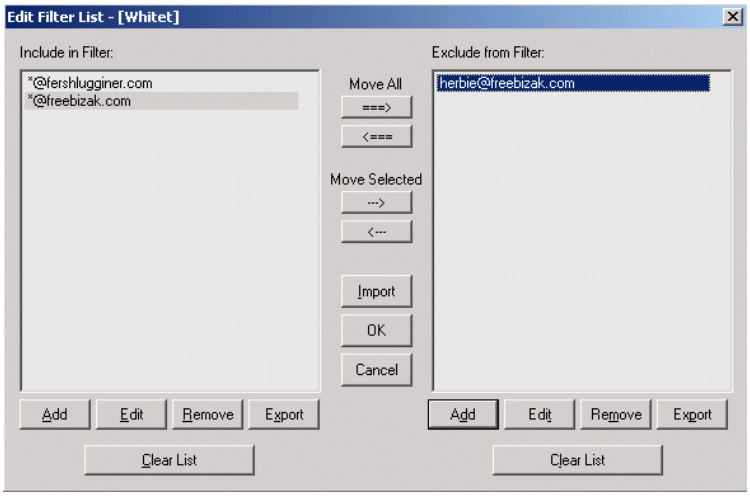
1. Click **Filter Lists** in the FILTERING shuttle.
2. Select **Keywords** in the List Types section.
3. Click **Add**, type a name for your new list, and then hit **ENTER**.
4. Click **Edit/Import** to edit the list. The Edit Filter List dialog appears, displaying all the current items in the left-hand column.
   - To add an item to the list, click **Add**, type in the text, and then hit **ENTER**.
   - To import a list of items in an external text file, click **Import**, and then select the file.
5. Click **OK** when you are finished creating the list.
6. Click **Save** to save your changes.

7. Select **Keyword** in the FILTERING shuttle. The Keyword Filtering dialog appears.
8. Select the IM Scan Job.
9. Select your new filter list in the Filter Lists section.
10. Set the Filter enabler to **Enabled**.
11. Set the **Action** for Antigen Here's how to take upon detecting a match to the filter criteria. The choices are: "Skip: detect only" (Records the number of files that meet the filter criteria, but allows the files to route normally), "Purge: eliminate message" (deletes the message), "Identify: tag message/file" (replaces the original message with the "Tag Text", which is set on the Scan Job Settings dialog, reached by clicking **Scan Job** on the SETTINGS shuttle).
12. Indicate if you would like to send Notifications and/or Quarantine identified files.
13. Indicate which messages this filter applies to: Inbound, Outbound, or Internal.
14. Specify how many different keywords must be matched in order for the Action to be taken, by using the **Minimum Keyword Hits** field. The default is one (1).
15. Click **Save** to save your changes.

Creating Allowed Sender/Recipient Lists

Antigen for IM provides allowed senders/recipients list functionality, so that you can maintain lists of "safe" IM Screen Names and IM Addresses that will not be subjected to filtering or spam scanning. Addresses of senders and recipients in the "From" or "To" field are checked against this list. If the e-mail address or e-mail domain appears on the list, Antigen will bypass all filtering and spam scanning that have been selected. Here's how to create an Allowed Sender/Recipient List:

1. Select **Filter Lists** from the FILTERING shuttle. The Filter Lists dialog appears.
2. Select **Allowed Sndr/Recp** from the List Types section.
3. Click **Add** in the List Names section, type a name for your new list, and hit **ENTER**.
4. Highlight the new list name, and then click **Edit/Import**. The Edit Filter List dialog appears. Enter IM addresses or Screen Names to include in the list, as follows:



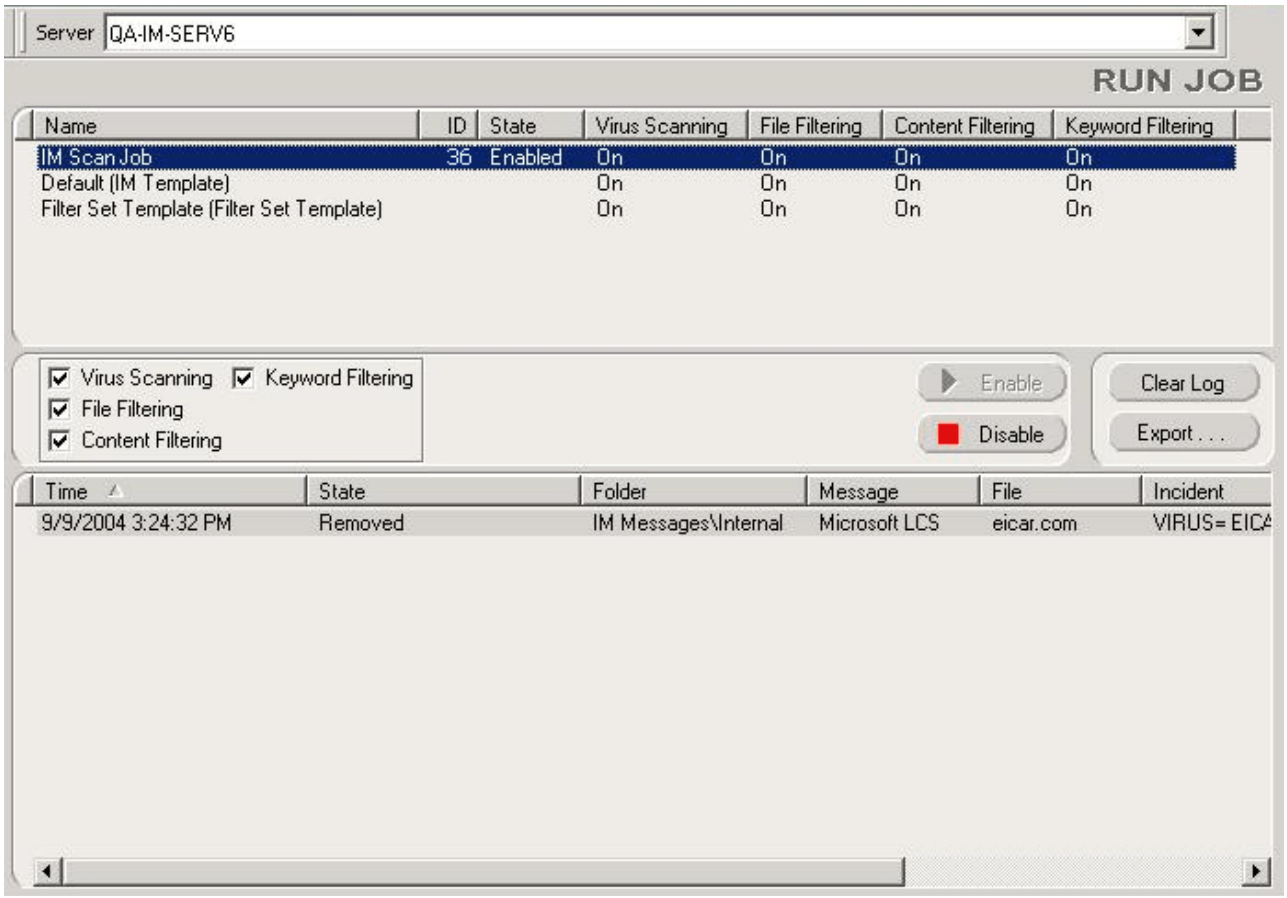
a. Click **Add** (under Include In Filter), enter the address or screen name, and then hit **ENTER**. Enter each address or domain individually.
b. To import a list of items in an external text file, click **Import**, and then select the file.
c. When you are done, click **OK** to return to the Filter Lists dialog.

5. Click **Save** to retain your work.
6. Select **Allowed Sndr/Recp** in the FILTERING shuttle. The Allowed Sender/Recipient dialog appears:
7. Select the IM Scan Job.
8. Select the new list in the Sender/Recipient Lists section.
9. Enable the new list by selecting **Enable** in the List State field.
10. Select the type of filtering that this list should apply to in the Skip Scanning Types section: content filtering, keyword filtering, and/or file filtering.
11. Click **Save** to save your changes.

Chapter 4 – Running the Scan Job

Now that you have installed and configured Antigen for IM, here's what you need to know about the IM Scan Job. For more detailed information on these procedures, see the Antigen For IM *User Guide*.

To see the status of the IM Scan Job, select **Run Job** in the OPERATE shuttle of the Sybari Client. The Run Job dialog appears:



Running the IM Scan Job

The IM Scan Job is always running, as long as two conditions are met:

1. You did not change the default value (“Enable”) for the **Enable Antigen** field in the General Options of the Sybari Client.
2. You did not disable the IM Scan Job on the Run Job dialog.

The **IM Scan Job** entry in the list of jobs at the top of the dialog shows its status. You can see, at a glance, if the IM Scan Job is enabled or disabled, and if it is performing virus scans, file filtering, content filtering, or keyword filtering, each of which can be controlled separately by means of the checkboxes beneath the Job List. (Any change to these scan settings will be performed “on the fly”, even if the job is currently running.)

Disabling the IM Scan Job

To disable the IM Scan Job, use the **Disable** button under the Job List. Enable it, once again, with the **Enable** button.

Checking Results and Status

The lower part of the Run Job dialog displays the infections or filtered results found by the currently-selected job. These results are stored in the virus log file by the AntigenService; it is not necessary to have the Sybari Client remain open.