IPSWITCH

IMail Server

Getting Started Guide

IPSWITCH

Ipswitch, Inc.
753 Broad Street
Suite 200
Augusta, GA 30901-5518

Web: www.imailserver.com
Phone: 706-312-3535
Fax: 706-868-8655

Copyrights

©1995-2008 Ipswitch, Inc. All rights reserved.
IMail Server Getting Started Guide

This manual, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by such license, no part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the expressed prior written consent of Ipswitch, Inc.

The content of this manual is furnished for informational use only, 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. also assumes no liability for damages resulting from the use of the information contained in this document.

Ipswitch Collaboration Suite (ICS), the Ipswitch Collaboration Suite (ICS) logo, IMail, the IMail logo, WhatsUp, the WhatsUp logo, WS_FTP, the WS_FTP logos, Ipswitch Instant Messaging (IM), the Ipswitch Instant Messaging (IM) logo, Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Other products and their brands or company names are or may be trademarks or registered trademarks, and are the property of their respective companies.

Update History

May 2001	First Edition
February 2003	Second Edition
March 2004	Third Edition
March 2005	Fourth Edition v8.2
November 2005	Fifth Edition v2006
January 2006	Sixth Edition v2006.02
April 2006	Seventh Edition v2006.04
July 2006	Eighth Edition v2006.1
February 2007	Ninth Edition v2006.2
October 2007	Tenth Edition v2006.22
February 2008	Eleventh Edition v10
November 2008	Eleventh Edition v10.02

CHAPTER 1 Getting Started with IMail Server

About Getting Started 1
Other Information Sources 1
Visit Our Web Site 2
Components of an Internet Mail System 2
IMail Support Center 3

Planning Your Installation

Step 1: What Do You Need? 5
IMail Server System Requirements 5
Step 2: Create DNS Entries for Your Mail Server 6
Setting Up DNS for the Primary Mail Host 7
Adding an Additional (Virtual) Mail Host 8
Setting Up DNS for Multiple Mail Hosts 8
Step 3: Choose the Type of User Database 9
Step 4: What E-mail Services Do You Want to Provide? 11
Step 5: Determine Security Levels and Access Control 12
SMTP Mail Relay options 12
SMTP Authentication 13
SSL for IMail Server and Web Messaging 13
Step 6: One Mail Domain (Host) or Multiple Domains? 14

Installing IMail Server

Step 1: Start the Installation and Activating IMail 15
Step 2: Set up your Web Server 16
Step 3: Set the Official Host Name for Your Server 17
Step 4: Select the User Database 17
Step 5: Set Security Options 18
Step 6: Select the IMail Services You Want to Use 19
Step 7: Final Options 20
Proxy Server 20
Start Menu and Shortcuts 20
Restart Your System 20
Instant Messenger User Database (IMail Premium Only) 20
WorkgroupShare Client Setup (IMail Premium Only) 21

Finalizing IMail Server Installation

Initial IMail Administration Server Login 23
- Restart Your System 23
- Initial IMail Administration Server Login 23
- Adding Administrators and Users to Your System 23

Remote Administration Access 25
Confirming your DNS Settings 25
Confirming Your IMail Server Installation 27
Confirming the User Database Setup 28
Sending and Receiving Mail in a Test Account 30
Upgrading 32
- Upgrading Using External Databases 32
- Upgrading the LDAP Database 33
- Upgrading Antispam Features 33

Uninstalling IMail Server 34

Using IMail Antivirus

About IMail Antivirus 35
IMail Antivirus Administration 35
Symantec Scan Engine Web Administrator 36
What's New with Scan Engine 5.2 36
New ScanEngine 37

Using IMail Antispam

About IMail Antispam 39
What You Can Do with the Antispam Features 41
Accessing the Antispam Features 42
Forwarding Spam to Ipswitch 44

Mail Servers and the DNS

What is DNS? 45
How a Mail Server Uses DNS 46
Setting Up Mail Server Records in the DNS 47
- Configuring Your Local Network DNS server 47

Index

CHAPTER 1

Getting Started with IMail Server

In This Chapter

About Getting Started 1
Other Information Sources 1
Visit Our Web Site 2
Components of an Internet Mail System 2
IMail Support Center 3

About Getting Started

This **guide** provides instructions for planning, installing, and testing your IMail Server software.

This includes instructions for IMail, IMail Plus, or IMail Premium installations, as well as guidance in installing optional components: Antivirus for IMail, Premium Antivirus for IMail, and Instant Messenger.

This **IMail Getting Started Guide** can be accessed online at:

- **http://docs.ipswitch.com/_Messaging/IMailServer/v10.02/GettingStarted/index.htm**.

-OR-

- **Start > All Programs > Ipswitch IMail Server > Documentation > IMail Getting Started Guide**.

Other Information Sources

The following is a list of resources that you can use to get help with IMail:

- **IMail Administration Server Help**. Help is always available by clicking **Help** in all Ipswitch products. It provides information about IMail configuration, advanced configuration, services options, mailing lists, and more.

This online help is also available online at:

http://docs.ipswitch.com/_Messaging/IMailServer/v10.02/Help/Admin/index.htm

- **Release Notes**. The release notes, located in the **Start** > **Programs** > **Ipswitch IMail Server > Documentation** folder, provide an overview of changes, known issues, and bug fixes for the current release. The notes also contain instructions for upgrading IMail Server and configuring external databases.

  These release notes are also available at:

  http://docs.ipswitch.com/_Messaging/IMailServer/v10.02/ReleaseNotes/index.htm (http://docs.ipswitch.com/_Messaging/IMailServer/v10.02/ReleaseNotes/index.htm)

- Microsoft Internet Information Services (IIS) Help. Use the IIS help for additional information about IIS setup and configuration.

Visit Our Web Site

For more information about Ipswitch products and services, visit the Ipswitch Web site at: **http://www.ipswitch.com**.

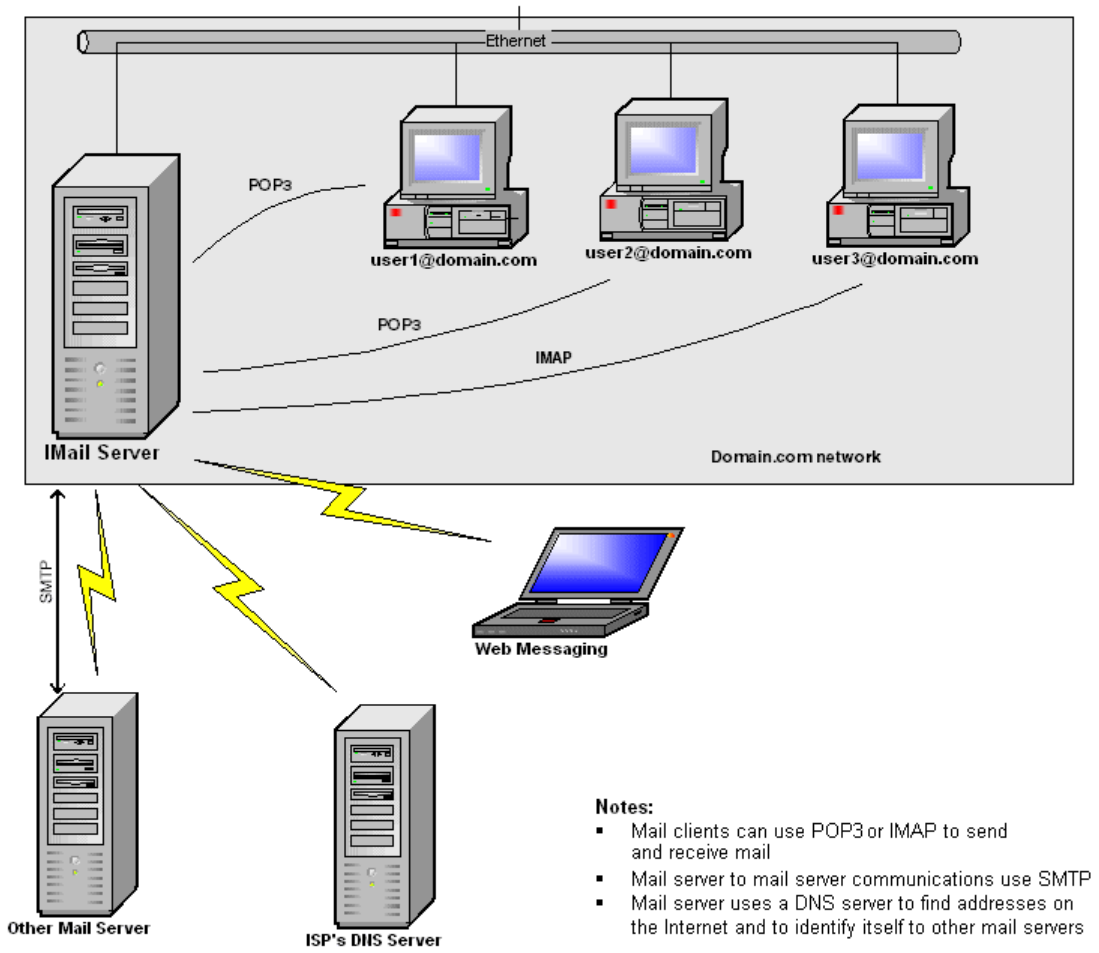
Components of an Internet Mail System

IMail Server provides the following basic services required to implement an Internet-based mail system:

- The SMTP server lets IMail Server communicate with other mail servers on the Internet.
- The POP3 server lets an e-mail client retrieve mail from the mail server.
- The IMAP server provides another method for an e-mail client to access mail on the mail server.

This guide focuses on setting up the mail server; however, you also need the following software components to connect your mail server to the Internet and to provide mail capabilities for your users:

- **Domain Name System (DNS) server**. The DNS server can be on your network or hosted by your Internet Service Provider.
- **E-mail client**. Users can use the Ipswitch IMail Web Messaging client to read and send mail via either a Web browser or proprietary e-mail client for each mail user, such as Microsoft® Outlook Express®, Microsoft® Outlook®, or Qualcomm Eudora®.



IMail Support Center

The IMail Support Center provides a number of resources including the following:

- User guides
- Domain Name System (DNS) help
- Access to product updates, utilities, Knowledge Base (KB) articles, and other IMail resources.
- Technical support information, such as e-mail support forums, service agreements, and licensing information.
- IMail user forum, which gives you an opportunity to interact with other IMail customers to share tips and tricks.

You can access the **IMail Support Center** at **http://www.imailserver.com/support (**http://www.imailserver.com/Support/**).**

CHAPTER 2

Planning Your Installation

If you have a working knowledge of Windows-based applications and operating systems, you will find that installing IMail Server is quick and easy. However, we recommend that you plan the installation to ensure an IMail Server configuration that works for your organization.

This section describes what you need to know about the primary host (the system on which you install IMail Server) and what decisions you need to make before running the installation.

In This Chapter

Step 1: What Do You Need? 5

Step 2: Create DNS Entries for Your Mail Server 6

Step 3: Choose the Type of User Database 9

Step 4: What E-mail Services Do You Want to Provide? 11

Step 5: Determine Security Levels and Access Control 12

Step 6: One Mail Domain (Host) or Multiple Domains? 14

Step 1: What Do You Need?

To get the best performance and the flexibility to expand your mail service, we recommend that you dedicate a computer to function as your e-mail server and that you do not run other servers on the computer.

IMail Server System Requirements

Hardware

- An Intel Pentium® 4, 1 GHz or higher or an equivalent processor. For best results, a Pentium4, 3+ GHz. For high mail traffic, use multiple processors.
- 512 MB RAM minimum; 1+ GB recommended.
- TCP/IP enabled NIC card with a **static** IP address.
- A broadband or dial-up connection to the Internet.
- Modem and phone line are required for mail-to-pager, mail-to-fax, and IMonitor notifications.

Note: For best performance, we recommend that you make sure the latest updates for the operating systems be employed. Additionally, we recommend NTFS (rather than FAT) file system for increased operability and security.

Tip: IMail Server runs properly on the minimum hardware requirements recommended by the installed operating system. Performance and capacity increases are based on processor speed, RAM, and drive space. As with all server applications, we recommend that you install IMail Server on the fastest and most powerful server that your budget allows.

Software

- Microsoft® Windows® 2000 Server or Microsoft Windows 2003 Server

Note: Do NOT deploy IMail on a Windows 2000 Domain Controller, or on a 64-bit OS. IMail Server has not been tested with 64-bit operating systems.

- Microsoft Internet Information Services (IIS) 5.0 or higher
- Windows Script 5.6 (part of Microsoft Internet Explorer 6)
- Microsoft Data Access Component (MDAC) 2.6 or later
- Microsoft® .NET Framework 2.0

Note: If you are missing any of the above, see the latest Release Notes for links to their sources.

Step 2: Create DNS Entries for Your Mail Server

Determine the Domain Name System (DNS) settings required for the system you will install IMail Server on. Before you create DNS entries, plan the following for your Windows TCP/IP settings:

- **Primary Host**. The server you install IMail Server on.
- **Host Name** (of Primary Host). The host name for your e-mail server, for example, mail.
- **IP Address** (of Primary Host). The IP Address is a static address for the e-mail server host (for example, *156.21.50.15*).
- **Domain Name**. The domain name identifies the network that the host is on (for example, domain.com).

To identify your mail host in the DNS, use the Host Name plus the Domain Name. For example, *mail.domain.com*. This is also known as the Fully Qualified Domain Name (FQDN).

To add the DNS information on a Windows 2000 system:

- Click the **System** icon in the Control Panel, select the **Network Identification** tab, then click **Properties**. The Identification Changes dialog box shows the domain information.

To add the DNS information on a Windows 2003 or Windows XP system:

- Click the **System** icon in the Control Panel, click **Network Connections** > **Local Area Connections** > **Properties**. Select Internet Protocol (TCP/IP) from the list, then click **Properties** > **Advanced** > **DNS** tab.

The Host Name and Domain must be registered in the DNS (Domain Name System) in order for your remote hosts (not on your local network) to communicate with your system.

Setting Up DNS for the Primary Mail Host

To properly send and receive e-mail, add the following records to your DNS server. If an Internet Service Provider (ISP) is hosting your DNS server, contact your ISP to have the appropriate records added to the DNS server.

- **MX Records**. Create a Mail eXchanger (MX) record to identify the host name of the computer running the mail server. If you plan to host multiple domains, you need an MX record for each domain. The MX record points to the (fully qualified) host name of the IMail Server (the Primary Host). For example: *domain.com* IN MX 10 *mail.domain.com*
- **A Records**. Create an Address (A) record for the IMail Server that has the IP address of the IMail Server (the Primary Host). The A record maps a host name to an IP address. For example: *mail.domain.com* IN A 156.21.50.15
- **PTR Records**. Create an A pointer (PTR) record for reverse lookups. You need a PTR record that resolves the IP address of your IMail Server (the Primary Host) to the Official Host Name of your IMail domain. For example: 156.21.50.15 in-addr.arpa. *host=mail.domain.com.*
- **SPF Records** (optional, but required for receiving mail servers to use SPF features). SPF records let other e-mail services use SPF filtering (if the feature is available on the mail server) to protect against incoming e-mail from forged (spoofed) e-mail addresses that may be associated with your mail server. As SPF records are implemented more widely, SPF filtering will become more effective at identifying spoofed e-mail messages. For more information, see the *IMail Administrator Help* or go to the SPF community at **http://www.openspf.org/Project_Overview.**

Example: The DNS entries for a host with an official host name of imailbox.domain.com would look like:

```
SOA
$ORIGIN
...
domain.com
IN MX 10 mail.domain.com                    (MX record)
mail IN A 156.21.50.5                       (A record)
5.50.21.156.in-addr.arpa.,type = PTR
host = mail.domain.com                      (PTR record)
```

A DNS lookup for mail sent to user@domain.com would find that the mail must be sent to the host at mail.domain.com.

Adding an Additional (Virtual) Mail Host

Note: Additional mail domains, virtual domains, and domain aliases can be added after the initial install. If added later, make sure that you update the DNS record according to the mail domain additions.

There are two types of virtual hosts:

- **Virtual hosts with IP addresses**. Recommended when you want IMail Server to receive mail for a second domain with its own users. You can set up a virtual host for the second domain. For example, if your mail server provides mail service for domain1.com, and you also want it to provide mail service for domain2.com, you can create a virtual host for domain2.com.
- **Virtual hosts without IP addresses**. Recommended when you have a shortage of IP addresses or when you want to forward all mail for a domain to a user at another domain.

Note: Whether you use a virtual host with an IP address or without an IP address, you must make DNS entries for your domain(s). See *Setting Up DNS for Multiple Mail Hosts* (on page 8).

For more information about Virtual Hosts, see the **IMail Administrator Help**.

Setting Up DNS for Multiple Mail Hosts

If you want to set up a virtual host **with** an IP address, make the following entries in your DNS:

- Add an MX record for the mail domain (for example, mail.domain2.com). The MX record identifies the host name of the virtual host.
- Add an A record for the host name of the virtual host. The A record maps a host name to an IP address.
- Add a PTR record for the IP address of the virtual host. The PTR record maps an IP address to the host name and is used for reverse lookups.

Example: The DNS entries for a virtual host with a host name of mail.domain2.com would look like:

```
SOA

$ORIGIN

...

domain2.com

      10.50.21.156.in-addr.arpa.,type = PTR

      host = mail.domain.com                    (PTR record)
```

A DNS lookup for mail sent to user@domain2.com would find that the mail must be sent to the host mail.domain2.com.

If you want to set up a virtual host **without** an IP address, make only one entry in your DNS: an MX record for the mail domain (for example, mail.domain3.com). This MX record identifies the host name of the primary mail host.

Example: The DNS entries for a virtual host without an IP address for which the host name is mail.domain3.com would look like:

```
SOA

$ORIGIN

...

domain3.com
```

A DNS lookup for mail sent to user@domain3.com would find that the mail needs to be sent to the host mail.domain.com.

Note: The MX record for a virtual host without an IP address does not have to use the primary mail host domain name; the MX record can also use domain names of other available hosts with an IP address.

For more information about setting up the DNS entries, see:

- A primer with examples in "*How a Mail Server Uses DNS* (on page 46)".
- DNS Help on the IMail Support Center at:

  http://www.ipswitch.com/Support/IMail/dns.html
- Our Knowledge Base for IMail Support Center at:

  http://www.imailserver.com/support/kb.html
  (http://www.imailserver.com/support/kb.html).

Note: You can use Ipswitch WS_Ping ProPack to look up DNS information. For more information about looking up DNS information using WS_Ping ProPack, see "Step 1: Confirm your DNS Settings" on page 23.

Step 3: Choose the Type of User Database

Identify the database that the Primary Host uses to register and authenticate users. The Primary Host can use one of the following databases for registration and authentication:

Note: Registration creates the user mail account and authentication verifies user IDs and passwords.

- **IMail Database**. All user IDs and passwords for mail accounts are stored separately, from either the Windows NT or Windows 2000 user database or other external database, or in a proprietary database in the Windows registry. This database is available, managed, and shareable only in support of the IMail or ICS applications.

  You can also import Windows NT or Windows 2000 users into an IMail user database without having them linked to the Windows NT or Windows 2000 user database. For more information on importing Windows NT or 2000 users, see the **IMail Administrator Help**.

- **Windows NT Database.** This database automatically creates user mail accounts for any user listed in the Windows NT or Windows 2000 user database on your host machine.

Caution: Don't use this option if on a domain - use Active Directory instead.

Note: The Primary Mail Host must have access to the Windows NT or 2000 user database for your network.

To view a current list of users, add users, or delete users in your Windows NT or 2000 user database, use the appropriate administrative tool (for example, Windows NT User Manager) as described in your Windows documentation. You cannot view, add, or delete NT database users with IMail Administrator.

Note: Windows NT database and Windows 2000 databases use different database administration tools.

A mailbox and other user files are created for a user when the mail server receives a message for that user or when a user first accesses the IMail Server through a mail client.

- **External Database**. IMail Server can use an external database to register and authenticate users. This option lets you specify an existing ODBC-compliant user database and lets you add and delete users either from the IMail Administrator or directly in the external database. IMail Server supports Microsoft SQL Server or Microsoft Access.

Important: If you use an external database, before you start the IMail or ICS installation, you need the ODBC System DSN name for the database and the User ID and Password to log on to the database.
IMAILSECDB is the default name that the IMail ODBC link uses. For example, for the ODBC System Data Source Name, enter: `imailsecdb;UID=imailuser;PWD=password`

Important: Before you use IMail Server Administrator to associate an external database with a host, use the ODBC Data Source Administrator to make sure there is a System DSN (Data Source Name) that points to a valid database name. See your Windows operating system and database documentation for information on the System DSN.

Note: If you want to use a different ODBC database, you can modify IMail Server's ODBCUser.dll file to support it. For more information, read the ODBC topics in our Knowledge Base at: **http://www.imailserver.com/support/kb**

To display the topics, enter **ODBC** in the **Search for** box, select *IMail Server* from the product list, then click **Search**.

- **Active Directory** - This database will create user mail accounts for all users in the Active Directory database as set by the Naming Context under **Domain Properties > User Database Type (NT/AD Database)**.

Important: To hide Active Directory users from the IMail Server, add the word "built-in" in the front of the user description.

Step 4: What E-mail Services Do You Want to Provide?

In addition to the basic SMTP service, IMail provides other services that you can start and stop at one source - the Service Administration page. Individual online help files are available that explain each service in more depth. Services provided with the installation are:

- **Symantec Antivirus Scan Engine** (available separately) provides automatic protection from viruses, worms, and trojan horses.
- **Bit-Defender Antivirus** (available separately). provides fully integrated proactive protection against viruses, trojans, or other potentially malicious codes.
- **Premium Antispam Service** (available with IMail Premium or IMail Plus) provides Commtouch Advanced Security Daemon (a.k.a. ctasd™) a plug-and-play email-borne spam and malware outbreak detection daemon that combines your current core messaging network infrastructure with advanced detection and classification capabilities.
- **IMail Web Calendar Service(Old Web Calendar)** lets users access Web Calendaring, which allows them to store schedules, set appointments, and send e-mail date reminder information using a Web browser. This service is still in place for access to the old Web Calendar which will be phased out and replaced with the new Web Calendar that no longer requires a service and works directly with the WorkgroupShare databases.

Note: The new Web Calendar does not require a service. It is controlled at the domain and user level for access.

- **Ipswitch Instant Messaging Server** (available with IMail Premium, or separately) lets users converse instantaneously and store past conversations.
- **POP3 service** lets users retrieve mail and send mail using clients like Qualcomm Eudora and Microsoft Outlook. With POP3, user mail is usually stored on the user's PC.

- **IMAP4 service** lets users read mail from the server and send mail using clients like Qualcomm Eudora, and Microsoft Outlook. With IMAP4, mail is usually stored on the mail server.

Note: IMail Web Client no longer uses IMAP, it accesses the mail server directly.

- **IMail Queue Manager Service** controls the flow of messages through the mail queue, and is a component of the SMTP delivery process.
- **IMail Sys Logger Service** lets users view the mail queue log files (also known as the Spool Directory).
- **LDAP service** uses a client/server architecture to publish user information (called "attributes") on the server and provide access to the information from LDAP-enabled clients.
- **Ipswitch WorkgroupShare Service** (available with IMail Premium) automatically imports contacts and contact lists from previous versions of Web Messaging or existing versions of Microsoft Outlook into the new IMail Web Messaging client.

Step 5: Determine Security Levels and Access Control

Identify the levels of security and access control needed to ensure the integrity of your mail server. IMail Server provides several ways to secure your e-mail server; for example:

- *SMTP Mail Relay options* (on page 12)
- *SMTP Authentication* (on page 13)
- *SSL for IMail Server and Web Messaging* (on page 13)

SMTP Mail Relay options

Mail relay occurs when IMail Server (or any SMTP server) accepts mail destined for another host and delivers it to that host. A message that originates on a computer other than the IMail Server host and destined for another host must pass through the IMail Server (i.e., IMail Server must relay the message). If your users (on the local network) use a POP3 or IMAP mail client to send mail via the local IMail Server, then IMail Server needs to relay mail for them. IMail Server allows for the following mail relay options (listed in order from most secure to least secure):

- No mail relay (install default)
- Relay mail for (Addresses)
- Relay mail for local hosts only
- Relay mail for local users only
- Relay mail for anyone

Local mail (destined for the IMail Server host or originating from the IMail Server host) does not use the relay function.

Note: During installation, you can select from four options: **Relay for select addresses**, **No mail relay**, **Relay mail for anyone**, and when upgrading: **Do not change my existing local mail relay settings**. After installation, you can change the relay setting in the **Services** tab > **SMTP Settings** page in IMail Server.

- **No mail relay** (recommended)

  The SMTP server will not accept mail destined for other hosts (any host not on the IMail Server machine) unless it comes from users who set their mail clients to do SMTP authentication. Make sure all mail *clients* are set up to SMTP Authenticate; otherwise, the client cannot send mail to non-local e-mail addresses. SMTP authentication means that the user name and password are presented to the mail server when the client sends a message.

- **Relay mail for anyone** (not recommended)

  The SMTP server accepts mail from any host that is destined for any other host, and redelivers that mail (i.e. becomes a mail gateway). This option is the least secure because it allows your server to be used by anyone to send mail to anyone. Some bulk mailers may take advantage of this capability to not only relay mail through your server, but to make it appear as if mail is originating from your server.

  If you select this option your server may be blacklisted for running an open relay. To prevent this you should select **Relay mail for (Addresses)**.

- There are several other mail relay options available after installation including **Relay mail for (Addresses)**, **Relay for local hosts only**, and **Relay for local users only**. **No mail relay** is the best option if you are unable to use **Relay mail for (Addresses)** because your users dial up using dynamic IP addresses.

For more information on Mail Relay options and other security features, see the **IMail Administrator Help**.

SMTP Authentication

For secure data communication, SMTP Authentication lets you verify each user who attempts to send mail through your mail server, as long as SMTP Authentication is enabled on the IMail Server. Users need to set their mail clients to do an SMTP login; for example, in Microsoft Outlook on the **Tools >Accounts > Mail > Properties > Servers tab** select the option **My outgoing mail server requires authentication**.

SMTP Authentication is used in the following cases:

- If you use the **No mail relay** option for SMTP relay.
- If you use the **Relay mail for (Addresses)** option, SMTP Authentication enables users who send from IP addresses that you do not list; for example, users who are traveling and do not have a static IP address.

SSL for IMail Server and Web Messaging

IMail Server and Web Messaging uses the Microsoft Internet Information Services (IIS) Secure Sockets Layer (SSL) feature to encrypt communications between the IMail Web client and server. To learn more about using SSL with IIS, see the IIS help information.

Step 6: One Mail Domain (Host) or Multiple Domains?

You can have multiple domains on one IMail Server system. This feature lets you provide separate mail services for separate organizations. Domains can be added to the IMail Server after you have completed the installation of the primary domain.

For information about setting up additional domains and information about other advanced configuration options, see the **IMail Administrator Help**.

CHAPTER 3

Installing IMail Server

In This Chapter

Step 1: Start the Installation and Activating IMail 15
Step 2: Set up your Web Server 16
Step 3: Set the Official Host Name for Your Server 17
Step 4: Select the User Database 17
Step 5: Set Security Options 18
Step 6: Select the IMail Services You Want to Use 19
Step 7: Final Options 20
Instant Messenger User Database (IMail Premium Only) 20
WorkgroupShare Client Setup (IMail Premium Only) 21

Step 1: Start the Installation and Activating IMail

Note: Log on to your Windows system as a System Administrator, or to an account with System Administrator privileges.

1 Back up your Windows registry. (Run regedit select Export Registry File from the Registry menu.)

2 Do one of the following:

- If you purchased an IMail Server CD, insert the CD into the CD/DVD drive. If the CD does not automatically start the installation wizard, click **Start > Run**, then enter the CD/DVD drive letter followed by autorun.exe. For example, enter D:\autorun.exe.
- If you downloaded the program from the Ipswitch Web site, double-click the downloaded file.

Note: If you are upgrading, you will need to visit *http://www.myipswitch.com/licensing* (http://www.myipswitch.com/licensing) for more information on managing licenses, and customer assistance.

3 Before the welcome screen appears a background registry checker runs to validate that all system requirements are in place. For assistance in locating download sites access the latest release notes at IMail Support Center at **http://www.imailserver.com/Support/** (http://www.imailserver.com/Support/)

4 The Welcome screen appears and provides the option to activate your software, view the release notes and this Getting Started guide. If you decide not to activate at this point you will have 30 days to do so, before the services will stop working.

If you purchased an IMail CD, the license key is included on the activation card. During the installation wizard, on the product activation dialog, you will have an opportunity to activate IMail. Enter your license key, then click **Next** to complete the installation.

- OR -

If you downloaded the IMail program from the Ipswitch Web site, the license key is displayed on a browser page and e-mailed to you. During the installation wizard, on the product activation dialog, you will have an opportunity to activate IMail. Enter your license key, then click **Next** to complete the installation.

5 Click **Next**, will display the License Agreement. After reviewing and accepting click **Next**.

6 The Select Features screen displays the components that can be installed. By default all are checked, uncheck features not desired. Then click **Next**.

Note: IMail Server does not present any optional components to install. If you have purchased additional products, such as Antivirus for IMail, separate instructions for those products purchased separately appear later in this Guide.

7 On the Choose Destination Location dialog, either accept the default directory path, or enter the directory where you want to install IMail Server or browse to the directory where you want to install IMail Server. Then click **Next**.

Caution: This directory must not be moved or renamed after installation.

Step 2: Set up your Web Server

Choose IIS User Account

1 If you have multiple Web sites configured in IIS, a dialog tells you that the Installation Wizard has detected multiple Web sites set up in IIS. Select the Web site to which you want to install the IMail Administrator and Client applications. The Web site you select from the list will be the default Web site you log into for access to Web Administrator and Web Client applications. Click **Next**.

2 Choosing the IIS User Account is selection screen asks you to choose between using the default IIS user IUSR_ComputerName, or gives capability to use a different user for setup.

If you select "Use a different user" option it takes you to another window to allow you to log to another username that is either an NT system user or an AD domain user before continuing. This option requires that you set user permissions manually. For detailed information regarding this and manually configuring IIS, see the Release Notes.

3 Next, the install dialog asks you to choose to either restart IIS and all dependent services automatically, or not. We recommend that you select **Yes** and have setup restart IIS, as well as all other dependent services, such as WWW, FTP, and SMTP.

Step 3: Set the Official Host Name for Your Server

This installation screen, **E-mail Domain Name (Official Host Name)** asks you to confirm or enter the official host name of your primary host for your IMail Server installation.

If you don't know the Official Host Name, see *Step 2: Create DNS Entries for Your Mail Server* (on page 6) in the *Planning Your Installation* (on page 5) section.

If multiple hosts are required, you can add other "hosts" and "virtual hosts" after completing installation of the primary host.

Step 4: Select the User Database

The next screen (**Database Options**) asks you to select the user database option you prefer. See *Step 3: Choose the Type of User Database* (on page 9) in the "Planning Your Installation" section. Select from the following database options:

- **Windows NT User Database** - IMail Server creates a user mail account for each user listed in the NT Database. Note that you will need to use the Windows NT User Manager to add or delete users. You cannot add or delete users from the NT database using IMail Administrator.
- **IMail User Database** - User IDs and passwords for mail accounts are created using IMail Administrator and stored in a database on the IMail server.
- **External Database (ODBC compliant)** - IMail uses an external database to register and authenticate users. Users that you add and delete using IMail Administrator will be added to and deleted from that external database and vice versa.

  Selecting **External Database**, you must specify the ODBC **System DSN** for the database, along with the user ID and password to log on to the database server. IMAILSECDB is the default name that the IMail ODBC link uses. For example, for the **System DSN**, you would enter: `imailsecdb;UID=imailuser;PWD=password`

Note: If a domain uses an external database, the Internet guest account (IUSR_<computer name>) must have full permissions set for the directory in which the database exists. For example, if the external database resides in c:\somewhere, then the Internet Guest Account must have full permissions to that directory.

- **Active Directory Database -** IMail Server will create a user mail account for each Active Directory user listed from the Root Directory Service Entry (DSE). You can change this default in the Web Administrator under **Domain Properties > User Database Type > NT/AD Database (Drop down List) > Naming Context**. You cannot add or delete users using the IMail Administrator with Active Directory.

Note: IMail Server is now designed to not display built-in Active Directory users. The word "built-in" must be added to the front of the full description under Active Directory user properties.

Step 5: Set Security Options

The IMail Server provides an SSL (Secure Socket Layer) capability that lets Web Calendaring clients connect more securely to the IMail Web Calendaring server. The SSL capability relies on keys stored in the Windows registry and automatically retrieved during the loading process of SSL Server.

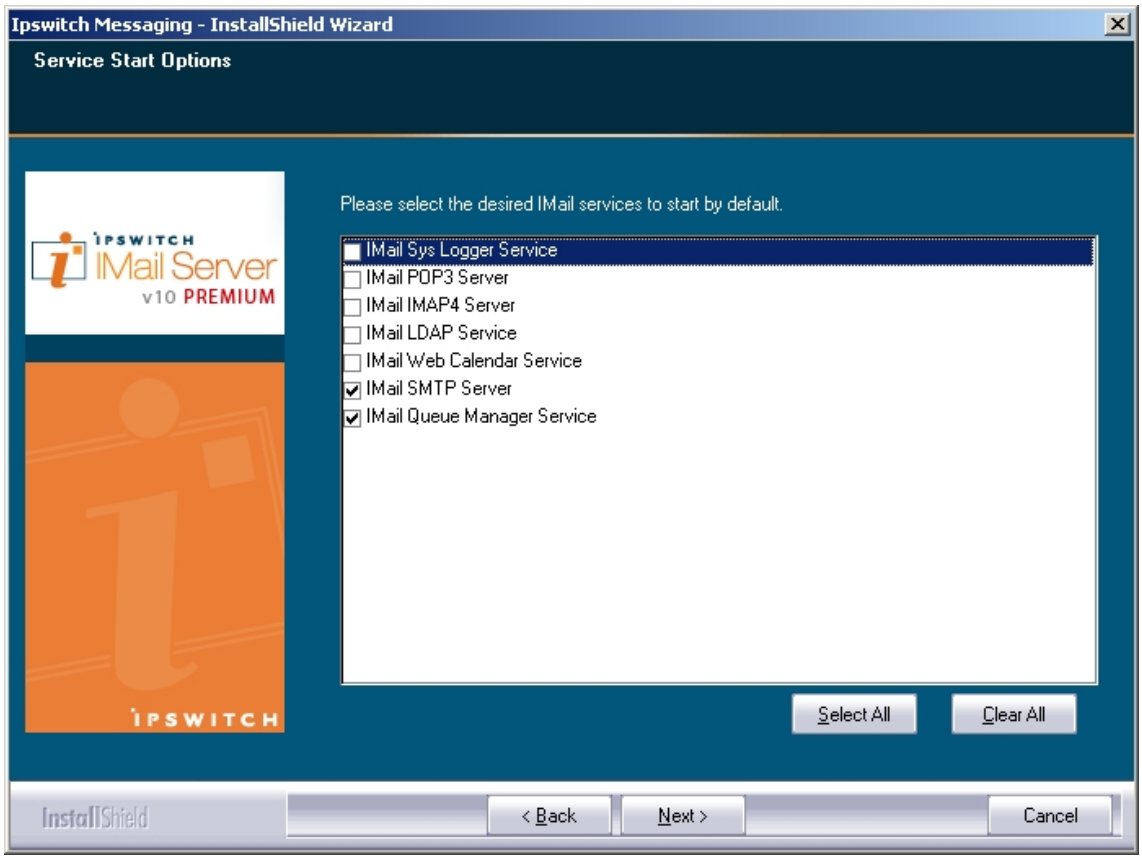
The next Setup Type screen, **Setting Default SSL Keys,** asks whether you want to install SSL by selecting one of the following options:

- **No,** if you already have a third-party SSL certificate. After installing IMail Server, click **Start** > **Programs** > **IMail Server** > **IMail Server > Mail SSL Configuration Utility**

- **Yes,** if you do NOT have a third-party SSL certificate, but want to run the IMail Web server using a “self-signed” SSL certificate.
- If you would like to read more about SSL before making a decision, click **No**. You can install default keys later.

Step 6: Select the IMail Services You Want to Use

On the Service Start Options screen, a list of IMail services already running on your IMail Server appears. If you have never installed IMail Server before, the pre-selected services are IMail SMTP Server and IMail Queue Manager Service. Select other services you want to start with IMail Server by default.



Note: You can also specify default services at any time after the installation. However, to send and receive e-mail, at a minimum, the **IMail SMTP, Queue Manager Services, and POP3 Server** boxes must be checked.

After you have selected Services, the Select Program Folder screen appears. Select the location where **Setup** is to create new shortcuts, and click **Next**. IMail Server is now configured and the installation finishes.

Step 7: Final Options

Proxy Server

If you are using a proxy server, enter the proxy server IP address and port in the text box provided. This will provide access to the messaging services. `Example: 196.168.100.55:80`

Start Menu and Shortcuts

Select **Start** > **All Programs** > and right click on **IMail Server Administration** to create shortcuts for your IMail Server installation. After creating the shortcut move the shortcut with your mouse to your desktop.

Restart Your System

If you are prompted to restart your system, it is because the installation could not properly set up a file. A Dynamic Link Library (DLL) is most likely to cause this problem. To ensure that IMail Server runs properly, restart as soon as possible.

Instant Messenger User Database (IMail Premium Only)

If you are installing IMail Premium then the Setup Type screen to select a user database for authenticating Instant Messenger Users will appear. The following options are:

- **Ipswitch Instant Messaging Server** - If Ipswitch Instant Messaging Server is selected, user IDs and passwords for IM accounts are stored and authenticated from the Ipswitch Instant Messaging database (in the registry).
- **Windows NT User Database** - If you select Windows NT User Database, Instant Messaging Server creates a user IM account for each user listed in the Windows NT Database user IDs and passwords for IM accounts are stored and authenticated from the Windows NT Database.

Note: With this option, you cannot add or delete users using IMail Server. NT User Manager must be used to add or delete users.

- **IMail Server (Default selection)** - Stores and authenticates all user IDs and passwords for IM accounts in the IMail Server database (in the registry).

Note: It is recommended that the IMail User Database be selected for user authentication.

WorkgroupShare Client Setup (IMail Premium Only)

The WorkgroupShare client must be installed on each computer that will share and use data, such as contacts and calendars, with Microsoft Outlook.

This Setup Type screen gives the option to share the WorkgroupShare ClientSetup folder located at:

`"C:\Program Files\Ipswitch\IMail\WorkgroupShare\ClientSetup"`, if default path was selected.

Ipswitch recommends sharing this folder across your network for client efficiency.

CHAPTER 4

Finalizing IMail Server Installation

In This Chapter

Initial IMail Administration Server Login 23
Remote Administration Access 25
Confirming your DNS Settings 25
Confirming Your IMail Server Installation 27
Confirming the User Database Setup 28
Sending and Receiving Mail in a Test Account 30
Upgrading 32
Uninstalling IMail Server 34

Initial IMail Administration Server Login

Restart Your System

After successful installation, some installations will prompt for you to restart your system. This is usually caused by the installation not setting up a file properly. A Dynamic Link Library (DLL) is most likely to cause this problem. To ensure that your IMail Server runs properly, restart as soon as possible.

Initial IMail Administration Server Login

After successful installation you will need to create a System Administrator, and possibly some test users. To do this, login as follows:

From the **Start** menu, select **Programs** > **Ipswitch IMail Server** > **IMail Server Administration**. The IMail Web Administration home page should appear.

-OR-

Open your web browser and enter "`http://localhost/IAdmin`". Localhost will bypass the login screen and take you directly to the IMail Web Administration home page.

Adding Administrators and Users to Your System

After successful login to the IMail Server, you will need to create a System Administrator, and possibly some test users.

Creating System Administrator

- Click **Manage Users** from the IMail Server home page. The User Administration page opens and displays users for the primary domain.
- Click **Add**, and the Add IMail User page will appear.
- Enter the following information:
  - **User ID**. Enter a unique user ID (user name) for the System Administrator. User IDs are limited in length to 1 to 30 characters and must be created from alphanumeric characters. The User ID cannot include spaces and must be a unique name within the domain you are adding the user to.
  - **Full Name**. Enter the user's First Name and Last Name.
  - **Password**. Enter a new password. Passwords are limited in length to 3 to 30 alphanumeric characters and cannot include asterisks.
  - **Confirm Password.** Enter the user password a second time to confirm the password.
  - **Allow Password Change** (selected by default). Allows user to change his/her password in Web Messaging.
  - **Grant Account Access** (selected by default). Select to let the user use the e-mail account remotely through POP3 or IMAP4. You can clear this option to disable the account without changing the user's password or removing him/her from the domain.
  - **Access Information Services** (selected by default). Select to make the user's LDAP information available in the LDAP database.
  - **Access LDAP Attributes** (selected by default). Select to let the user modify his/her LDAP attributes (name, address, organization, etc.).
  - **Allow Web Calendaring.** Select to let a user access IMail Web Calendaring (if it is installed).
  - **Allow Use of Ipswitch Instant Messaging.** (Only present if Ipswitch Instant Messaging is installed). Select to let the user have access to Instant Messaging. Clear the check box to disable the user's access.
  - **Allow Web Access** (selected by default). Select to let a user access his/her IMail Web Messaging client.
  - **System Administrator Permissions** (cleared by default). Select to allow full administration capabilities with all IMail features and options. System Administrators have Domain Administrator and List Administrator permissions.
- Click **Save** to create user, and return to User Administration page listing all users

Remote Administration Access

A valid user ID with System Administrator permissions must exist on your IMail Server, to allow remote login. Once a System Administrator is setup, remote access is readily available using your web browser.

To access the IMail Web Administration system remotely:

Enter the URL as follows: `"http://IP Address/IAdmin"`

-OR-

After your DNS configurations are complete the URL can be entered as: `"http://Domain Name/IAdmin"`.

Confirming your DNS Settings

This chapter provides some quick tests to ensure that you have a working IMail Server configuration. See How a Mail Server Uses DNS for detailed DNS information. To check the DNS record for your IMail Server, you can use either of the following tools:

- **WS_Ping ProPack**. If you have installed an evaluation copy of WS_Ping ProPack, you can use the Lookup tool that is a part of this suite of diagnostic tools.
- **Nslookup**. You can use the "nslookup" command in Windows 2000, Windows 2003, Windows XP.

To check your DNS settings using WS_Ping ProPack:

1. From the **Start** menu, click **Programs** > **WS_Ping ProPack** > **WS_Ping ProPack**, then click the **LookUp** tab.
2. View the **MX record** to verify that the domain name is pointing to the correct host name. Enter the following:
   a) **Name or IP address.** Enter the domain name (for example, domain.com).
   b) **DNS Server.** Enter the host name or IP address of the domain name server you want to use.
   c) **Query Type.** Select MX from the list.
   d) Click **Start.** You receive information such as:

```
>domain.com,
10,mail.domain.com
```

3. View the **A record** and verify that host name is pointing to the correct IP address. Enter the following:
   a) **Name or IP address**: Enter the Official Host Name of the IMail Server host (for example, **mail.domain.com**).

b) **DNS Server**: Enter the host name or IP address of the domain name server you want to use or select **stack** from the drop-down list to use your operating system's network stack.

c) **Query Type**: Select **A** from the list.

d) Click **Start**. You receive information such as:

```
>mail.domain.com
 156.21.50.10
```

4 View the **PTR Record** and verify that the IP Address points to the official host name. Enter the following:

a) **Name or IP address**: Enter the IP address of the IMail Server host (for example, *156.21.50.10*).

b) **DNS Server**: Enter the host name or IP address of the domain name server you want to use or select **stack** from the drop-down list to use your operating system's network stack.

c) **Query Type**: Select *PTR* from the list.

d) Click **Start**. You receive information such as:

```
 >10.50.21.156.in-addr.arpa.
host = mail.domain.com.
```

5 Record any errors. If you host your own DNS server, correct the entries. If your DNS service is hosted by an ISP, contact them and request the changes.

To check your DNS settings using the "nslookup" tool:

1 Run the Windows "nslookup" command to view the **MX record.** View the **MX record** to verify that the domain name is pointing to the correct host name. For example, enter:

```
nslookup
>ls -t MX domain.com
```

The command returns information such as:

```
>domain     MX 10   mail.domain.com
```

2 Under the Windows "nslookup" command, view the **A record** and verify that host name is pointing to the correct IP address.

```
nslookup
>ls -t A mail.domain.com
```

The command returns information such as:

```
>mail.domain.com  A  156.21.50.10
```

3 Under the Windows "nslookup" command, view the **PTR Record** and verify that the IP Address points to the official host name.

```
nslookup
>ls -t PTR 156.21.50.10
```

The command should return information such as:

```
>mail.domain.com  PTR  156.21.50.10
```

4 Record any errors. If you host your own DNS server, correct the entries. If your DNS service is hosted by an ISP, contact the ISP to request the changes.

Confirming Your IMail Server Installation

Note: When you start the IMail Server Administrator for the first time, (if you are using Internet Explorer in Microsoft Windows 2003), an "Internet Explorer Enhanced Security Configuration is enabled" browser screen may appear. If this screen appears, click the link to learn more about the browser's enhanced security configuration options. You may need to add IMail Server Administrator's URL to the inclusion lists in the Local intranet or Trusted sites zones.

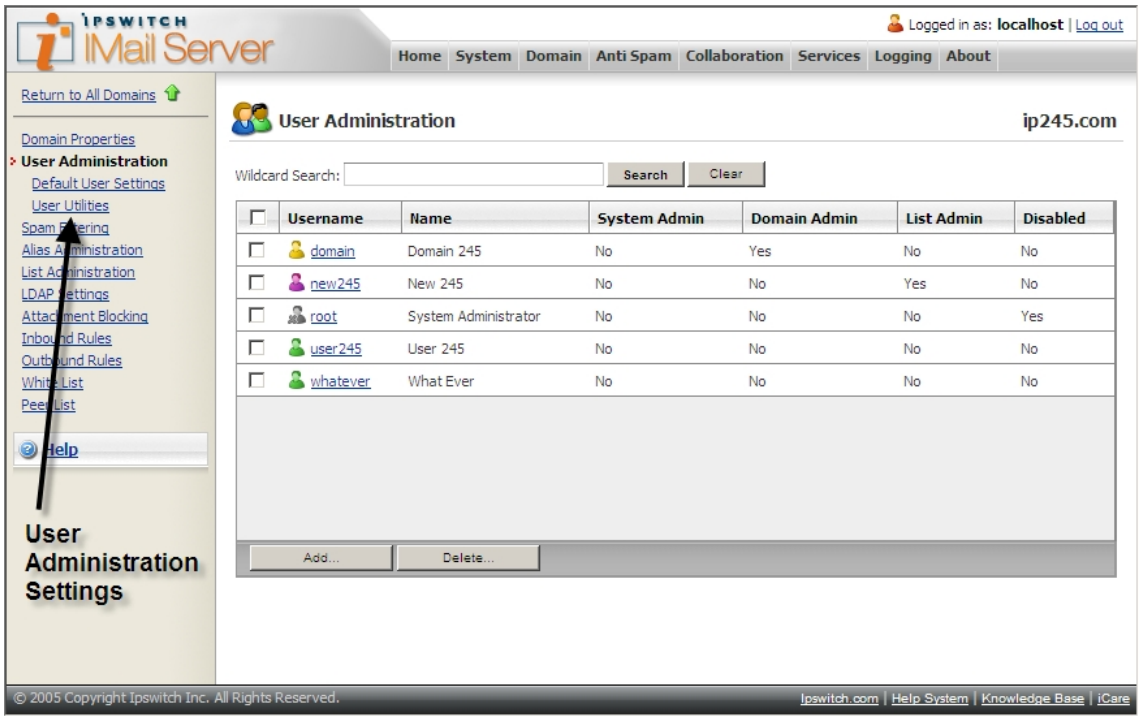
To confirm your IMail Server installation, do the following:

1 From the **Start** menu, select **Programs** > **Ipswitch IMail Server** > **IMail Server Administration**. The IMail Web Administrator home page will appear.

-OR-

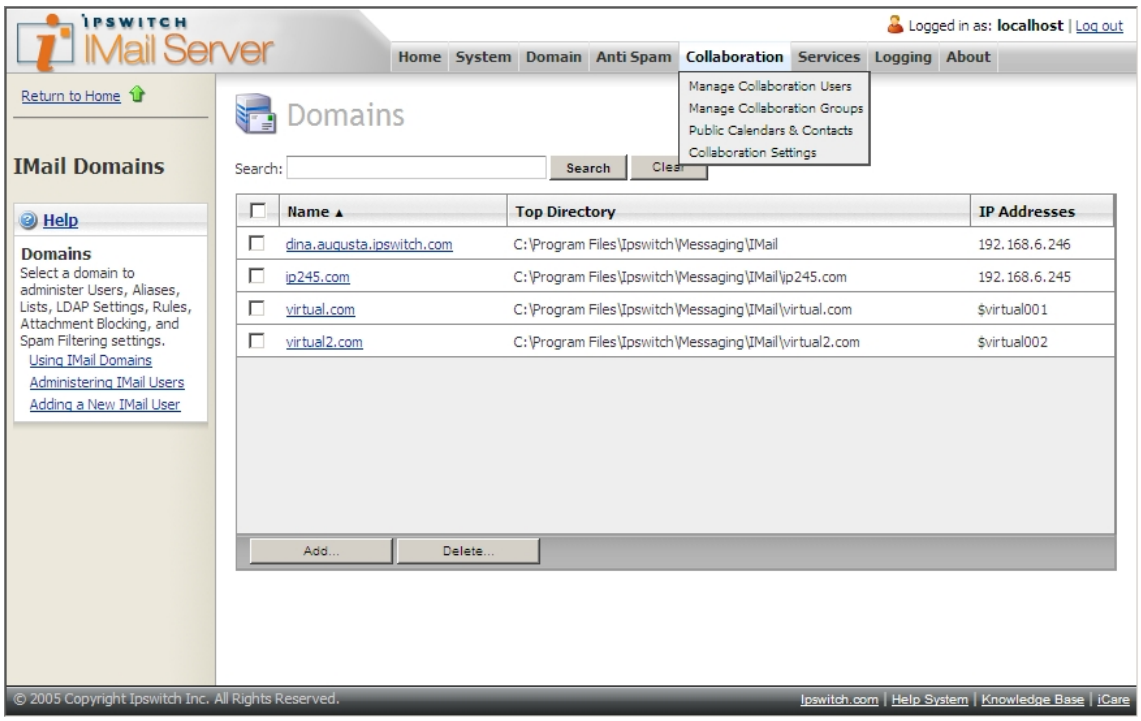
Open your web browser and enter the following URL: "`http://localhost/IAdmin`". The IMail Web Administrator home page will appear.

2 The **IMail Server Administrator** page provides a list of common administrator tasks. You can select a task or click a tab to access server administration options. If you select a tab, a left navigation bar displays links to tab related options. Click a link on the left navigation bar to drill down into related administration pages, as in the User Administration page illustrated below.



3 Click **Manage Domains**. The Domains page opens and displays a list of available mail domains.

-OR-



Mouse over the **Domain** tab. The default mail domain (or most recently selected mail domain) appears in the Domain tab list. If you want to change to another mail domain, click **Manage Domains**.

4 Click the mail domain that you set up as the **primary host** (for example, mail.domain.com). The **Domain Properties** page opens. Check the following:

- **Domain Name (Official Host Name** or **OHN**). Make sure this name matches the host name for the computer upon which you installed IMail Server.
- **Domain Alias(es) (Host Aliases)**. If you want users on the primary host to get messages addressed to the domain name, create an alias for the host.

Note: For more information about configuring the Mail Domain Configuration see the **IMail Administrator Help**.

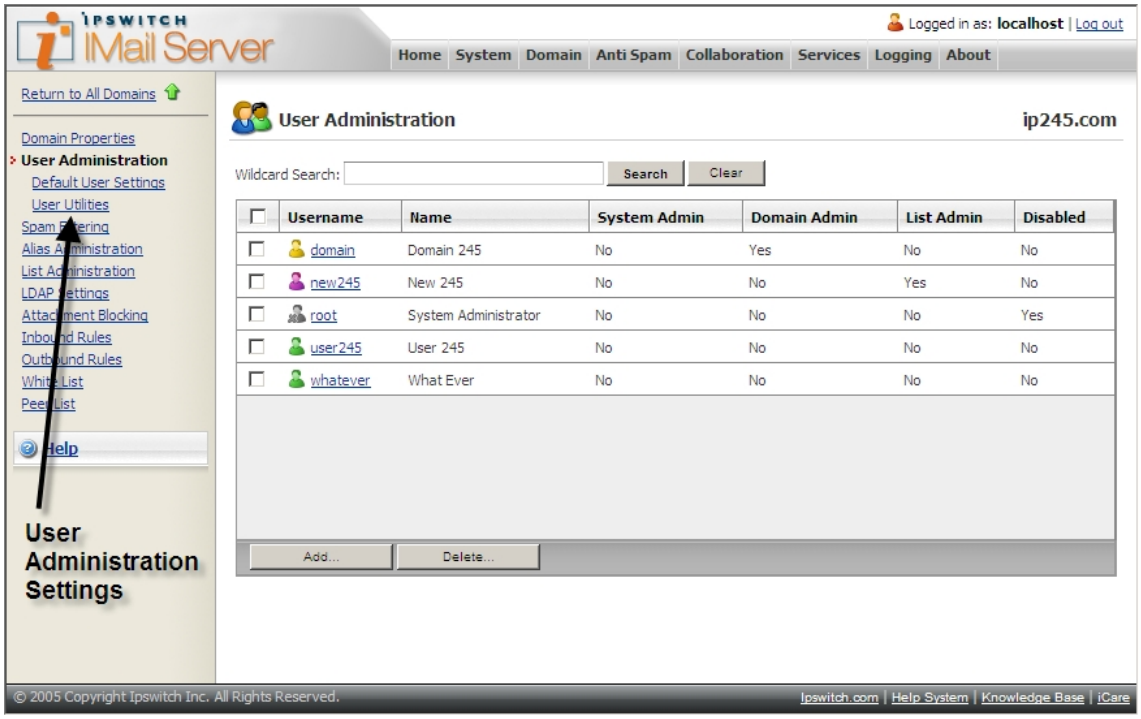
Confirming the User Database Setup

To verify that you can send and receive mail, you should have at least one user set up on the primary host.

Note: If your primary host uses the IMail user database, you may have created a user during the installation.

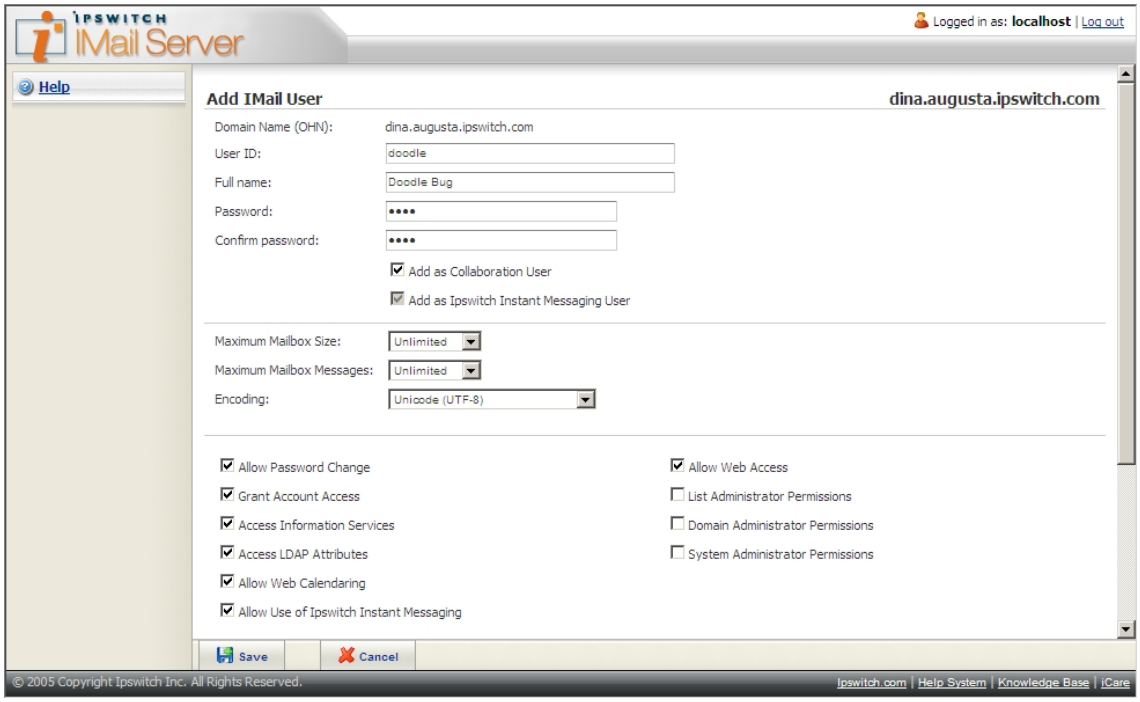
Make sure IMail users were created in the IMail user database:

1 With the primary mail domain (host) selected, as described in the *Confirming Your IMail Server Installation* (on page 27), click **User Administration** in the left navigation bar. The User Administration page opens.



If you only have a **root** user, perform the following steps to add a test user:

2 Click **Add**, then enter the user information in the Add IMail User page. A User ID must be 1 to 30 characters with no hyphens or spaces.



3 Click **Save** to add the user. The User ID is added to the list of registered users for the primary host.
If you want to view or change a user's settings later, click a user in the Username list on User Administration page.

If your primary host uses the Windows NT or Active Directory user database, you should have two default accounts: Administrator and Guest. If you need to add a user for test purposes, add the account in the appropriate Windows administrative tool.

Note: Windows NT database and Windows 2000 database use different database administration tools. To view a current list of users, add users, or delete users in your Windows NT or 2000 user database, use the appropriate administrative tool (for example, Windows NT User Manager, or Active Directory users and computers) as described in your Windows documentation. You cannot view, add, or delete users with IMail Administrator.

If your primary host is based on an external database and the external database is not populated, perform these steps:

1 In the IMail Administrator, go to the primary host's Username list on the User Administration page.
2 Add a few users.

The users you added can receive mail through IMail Server at the host name specified in Windows. For example, if you added the user **john** and the host name is **mail.domain2.com**, the user can receive mail addressed to **john@mail.domain2.com**.

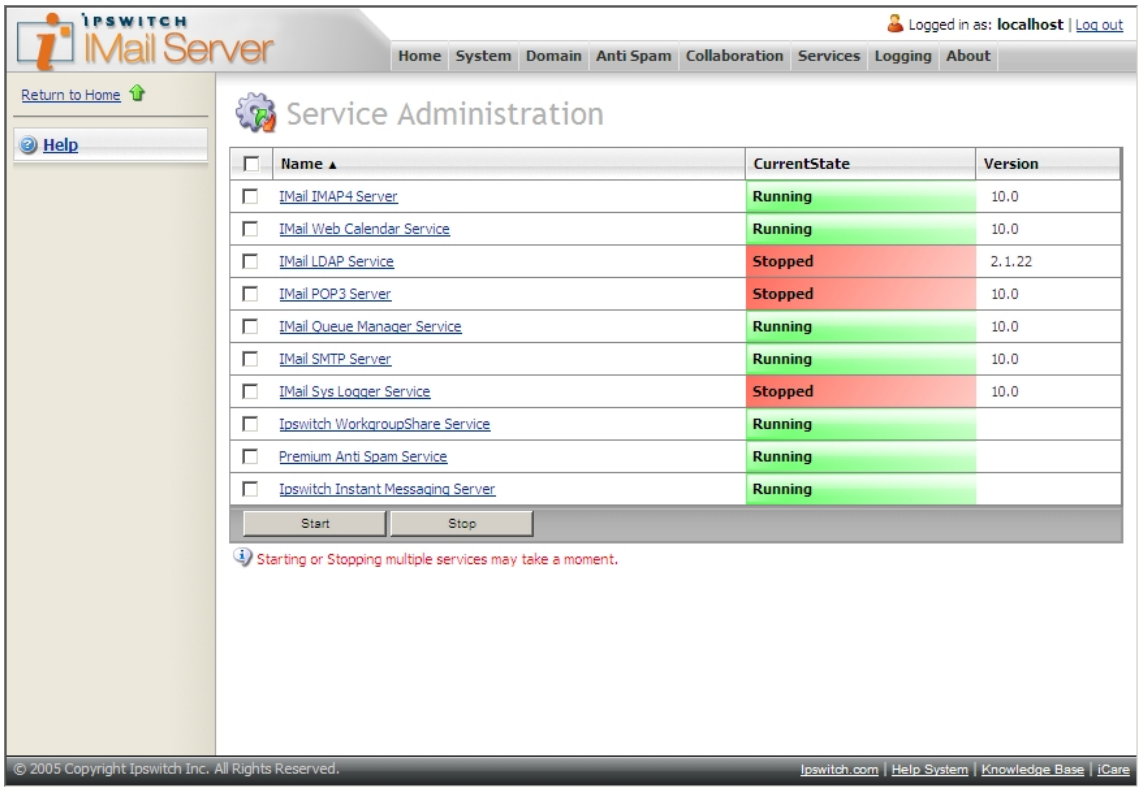
Note: If you want users on the primary host to receive messages addressed to just the domain name, create an alias for the virtual host. For example, if you want the user shown above to receive mail addressed to **john@domain2.com**, create a domain alias (host alias) of **domain2.com** for **mail.domain2.com**. For more information about configuring IMail Server, see the Mail Domain (Host) Configuration information in the **IMail Administrator Help**.

Sending and Receiving Mail in a Test Account

To send and receive mail in a test account, complete the following steps:

1 Check to make sure the mail services are running.

2 Click the **Services** tab and enter your network username and password. The Service Administration page opens.



3 Check to see if the SMTP, POP3, and IMAP4 services are running. The status displays in the **Current State** column. The SMTP status starts automatically and should be **Running**. If the POP3 and IMAP4 are not **Running**, then select the check box next to each service and click **Start**.

4 Start your e-mail client.

5 If you are using IMail Web Messaging (Web client), start your Web browser, then enter **http://localhost/IClient/** (only works when accessing local box)

-OR-

http://<IMail Server hostname>/IClient/
For example:
http://123.100.100.80/IClient, then press **ENTER.** The Ipswitch Web Admin login page appears.

6 Log on using one of the user accounts you created and send mail to another user. Then check that the mail appears in the e-mail recipient Inbox.

Caution: A version of IMail Client console application is installed with IMail Server. It is useful for reading the "root" mailbox, working with seldom-used accounts, and testing. The IMail Client application should *not* be used on the IMail Server to view end-user mailboxes because it can cause problems with remote access to the same mailboxes (depending on the user's remote client software).

7 Send a test message to test mail service to a remote e-mail address outside of the local network. If you are connected to the Internet, send mail to *imailtest@ipswitch.com*.

8 When you are satisfied that the mail server works properly, add e-mail domains (hosts) and users as needed.

Upgrading

This section is for users who are upgrading from a previous version of IMail Server. IMail Server is automatically installed in the same directory where you had the previous version or evaluation version. This directory should *not* be changed, moved, or renamed.

1 Back up the registry key, `HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail` (**Start > Run > enter regedit** locate this key and select **Export Registry File** from the **Registry** menu.)
2 Follow the same instructions used for new installations.

Note: Make sure that you stop all IMail services and close the IMail Administrator interface before upgrading.

In This Section

Upgrading Using External Databases (on page 32)

Upgrading the LDAP Database (on page 33)

Upgrading Antispam Features (on page 33)

Upgrading Using External Databases

When re-installing IMail Server over an earlier version, in which one or more hosts use an external user database, new columns must be added to the database tables. This is due to additional user-level data that must be stored for use with the Web Calendaring features. The new columns must be added to the user table for each IMail Server host that uses an external database.

If you are using Active Directory (AD) as your user database, it is strongly recommended that you use the Active Directory option on the configuration screen. This new option provides much better support for AD, provides for better security on your Web server, and offers greatly improved performance.

During the install, IMail Server determines whether your system currently uses an external database. If the answer is yes, then a dialog provides the following three options:

- Click **Yes** to have this install program automatically add the columns to all external database tables used to store IMail Server user settings.
- Click **No** to continue installation without updating the tables.
- Click **Cancel** if you want to manually add the necessary columns. The required columns can be found in the release notes. You will need to restart this install program when ready.

Warning: If you click **No** and install anyway, be advised that IMail Server may not function properly.

If a custom ODBC driver was used with a previous version of IMail Server, the driver must be modified to use the new columns. Source code for the basic ODBCUser.dll driver (tailored for SQL Server and Access) can be downloaded from the IMail Support Center at:
ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/odbcuser.dll
ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/odbcuser.dll

Upgrading the LDAP Database

IMail 8.1 and later use the OpenLDAP implementation. If you have an existing LDAP database with information that you want to retain after the upgrade, take the following precautions. Otherwise, your existing LDAP information will be deleted.

- Backup your LDAP database before upgrading. To access the LDAP database, enter the location of the directory where the OpenLDAP files are located. By default, the installation path for ICS is C:\Program Files\Ipswitch\Collaboration Suite\IMail\OpenLDAP. The installation path for IMail is C:\Program Files\Ipswitch\IMail\OpenLDAP. The following folders are located under the ...\OpenLDAP folder:
  - **bin**. Folder where all OpenLDAP binaries are stored.
  - **Openldap-data**. Folder where all folders with domain specific databases are stored. Each folder is named after each existing domain.
  - **schema**. Folder where all OpenLDAP schema files are stored. Schema files are text files that determine the properties of each object.
  - **Share\ucdata**. Contains supporting data files for the LDAP server. These files should not be modified.
- Clear the **Access LDAP Attributes** option before upgrading. To access this option in IMail Administrator, mouse over the **Domains** tab, click **User Administration**, then in the left navigation bar click **Standard User Settings**. The Standard User Settings page opens. Click to clear the **Access LDAP Attributes** option before upgrading.

Warning: If you click **No** and install anyway, be advised that IMail Server may not function correctly.

Upgrading Antispam Features

If you have previously installed IMail Server, you need to decide whether to overwrite the *antispam-table.txt* file. During installation a dialog is displayed giving you the following options to overwrite the existing *antispam-table.txt* file.

- **Merge.** Adds new words to your existing file. Does not delete or alter any existing entries.

- **Overwrite.** Overwrites your existing file. Note that if you have added words or changed word values in this file, these will be overwritten or deleted.
- **Ignore.** Does not modify the file.

Note: You can manually merge the new word counts into your current *antispam-table.txt* file after installation, using the antispamseeder.exe utility. For more information see the **IMail Administrator Help**.

Uninstalling IMail Server

To remove IMail Server, use the **Add/Remove Programs** applet in the Windows Control Panel. The following occurs:

- IMail services are removed from the Control Panel Services.
- Everything is deleted in the Windows registry under HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail (but the Ipswitch key is not removed).
- Directories and files created by the setup.exe are removed if nothing has been added to them. For instance, if you have not added users (and *root* never gets mail), the *Users* directory is removed.

Note: Removing IMail Server as described above does not delete the IMail directory or the subdirectories and files it contains. To remove these, you must delete them manually.

CHAPTER 5

Using IMail Antivirus

In This Chapter

About IMail Antivirus 35
IMail Antivirus Administration 35
Symantec Scan Engine Web Administrator 36

About IMail Antivirus

If you purchased IMail Secure Server or ICS Premium releases 2006.1 or prior, your mail server includes Symantec's ScanEngine, one of the most comprehensive virus scanners available. As of release 2006.2 of the IMail product family, Premium Antivirus for IMail (Symantec's ScanEngine) is now available separately but still integrates seamlessly with IMail.

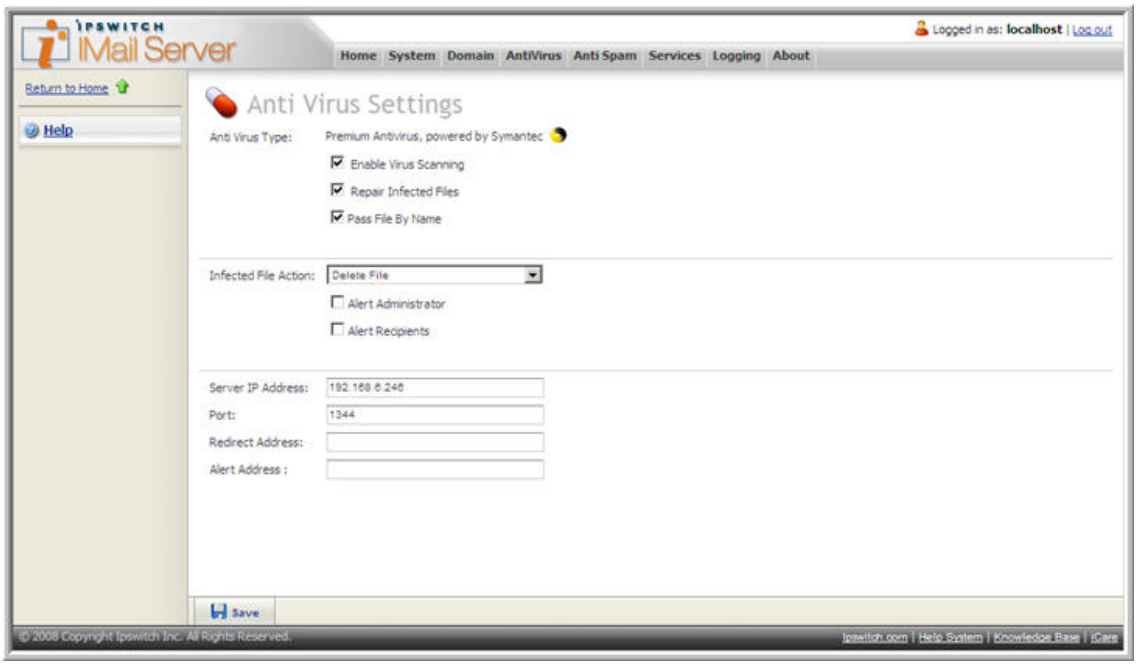
IMail Antivirus searches all incoming and outgoing mail for viruses, worms, trojan horses, and other destructive code. It does this by comparing all mail messages with a list of file extensions and known virus definitions.

It also uses heuristic technology to discover new viruses by searching for general characteristics of existing viruses. If it detects a virus, IMail Antivirus can attempt to repair the infected file, delete the message, or send a bounce message back to the sender. A log file entry is generated and an e-mail is sent to alert the administrator of the problem. In addition, the System Administrator can set a "Redirect Address" to send infected e-mail messages to. You can optionally send a message to the intended recipients informing them that the message could not be delivered.

IMail Antivirus Administration

You can administer IMail Antivirus configurations from:

- **IMail Administrator**. Click the IMail Administrator **Antivirus** tab. The Antivirus Settings page opens.



Use this page to enable virus scanning; set actions on infected files; configure the Antivirus server IP address, port, and redirect and alert e-mail addresses. For more information, see the **IMail Administrator Help**.

Symantec Scan Engine Web Administrator

You can access Symantec's Scan Engine protocols and administration settings through Symantec Antivirus Scan Engine Web Administrator. You can access the Scan Engine Web Administrator at the IP address entered in the **Proxy Server IP Address** on the Antivirus Settings page followed by :8004 (the default port for the Scan Engine Web Administrator).

For example:
http://123.100.100.80:8004. The default password for the Scan Engine Web Administrator is **admin**. The Symantec Antivirus Scan Engine Administration page appears.

What's New with Scan Engine 5.2

- Improved performance through changes to default tuning parameters.
- New Java and .NET API's (in addition to current C++)
- Rapid release anti-virus definition support
- Resource consumption reporting including details on:
  - Running threads
  - Scan statistics

- Number of processors in use by scan engine
- Log file size and available disk space

Previous Scan Engine changes:

- Scanning now uses ICAP mode on port 1344 rather than Native mode on Port 7777.
- Scan Engine admin now requires SSL on port 8004.
- The admin no longer uses a username. Only a password is required. If the password is not set during installation then access is not restricted.

New ScanEngine

You can customize a number of Antivirus settings in the Symantec Antivirus Scan Engine Web Administrator such as:

- HTTP bind address for the IMail Antivirus Server
- HTTP port number that the IMail Antivirus Server runs on
- Scan Engine Web Administrator password
- Type of information to log
- For more information, click **Help** in the Symantec Antivirus Scan Engine Web Administrator.

CHAPTER 6

Using IMail Antispam

In This Chapter

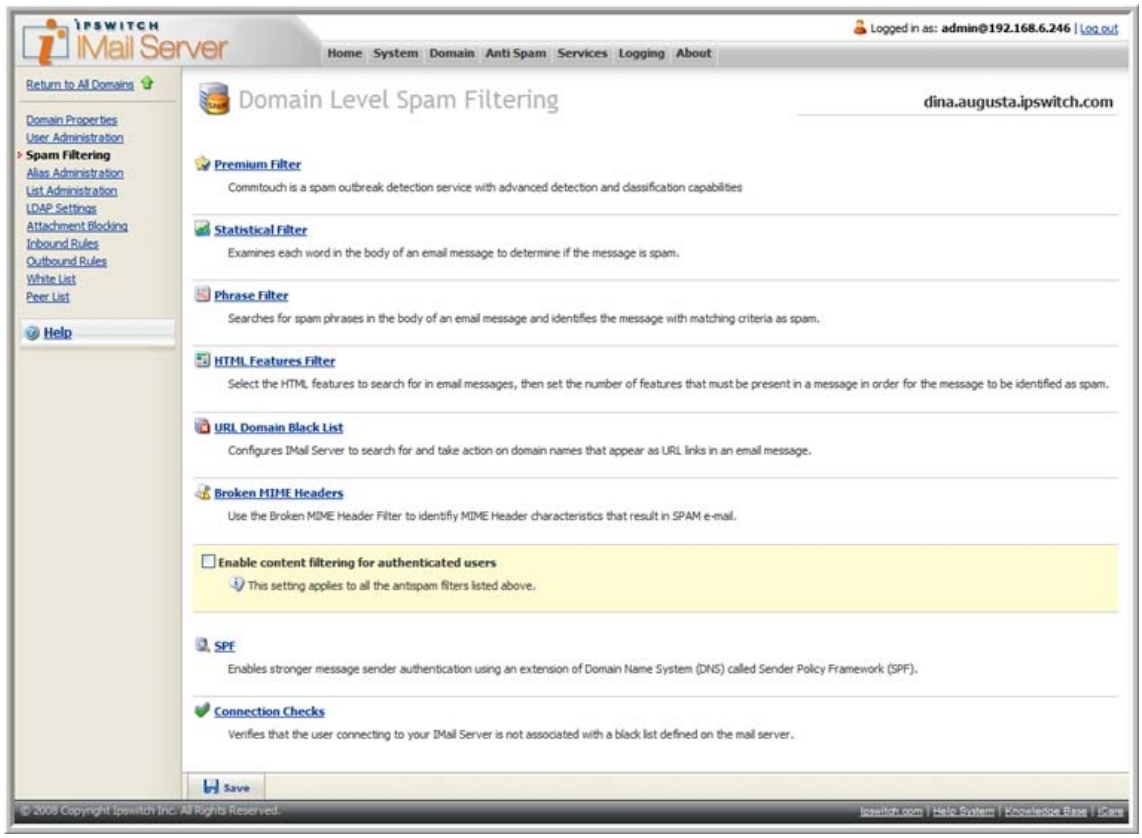
About IMail Antispam 39
What You Can Do with the Antispam Features 41
Accessing the Antispam Features 42
Forwarding Spam to Ipswitch 44

About IMail Antispam

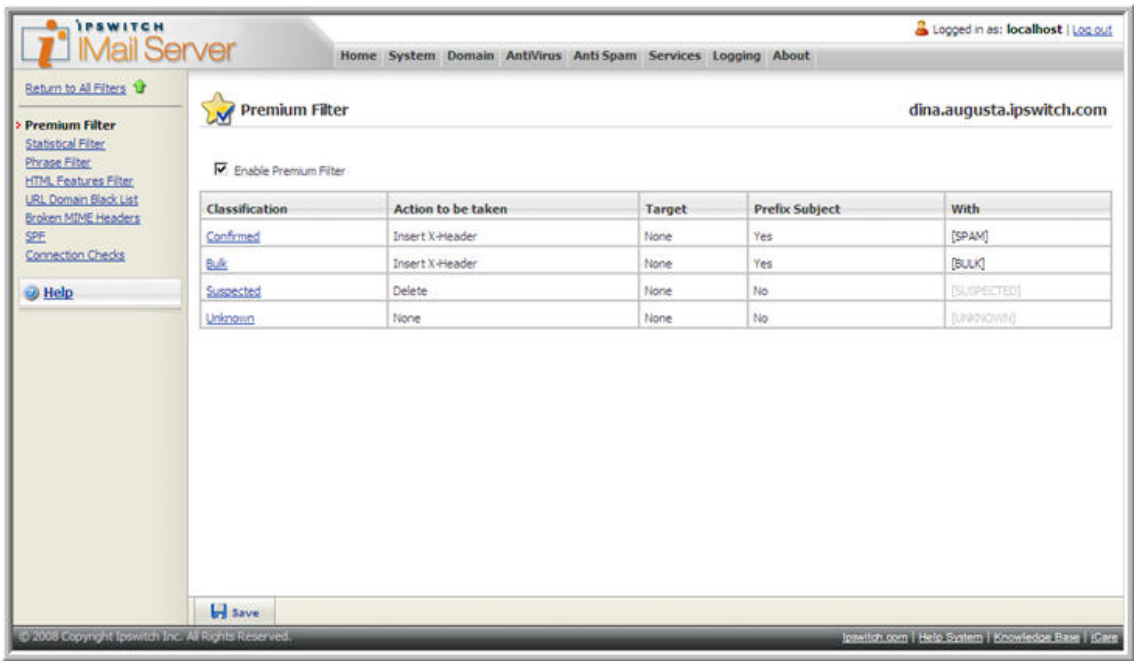
IMail Premium and IMail Plus editions include Premium Antispam technology. Commtouch Advanced Security Daemon (a.k.a. ctasd™) is a plug-and-play email-borne spam and malware outbreak detection daemon that combines your current core messaging network infrastructure with advanced detection and classification capabilities. The daemon adds a layer of e-mail filtering to your mail delivery system in order to provide real-time classification, already in the first minutes after a new outbreak is launched.

All members of the IMail product family include standard antispam features. The antispam features are custom configured by the administrator to identify spam and prevent it from clogging your inbox. Mail messages are passed through several layers of filters and tests to assure that maximum spam detection is achieved.

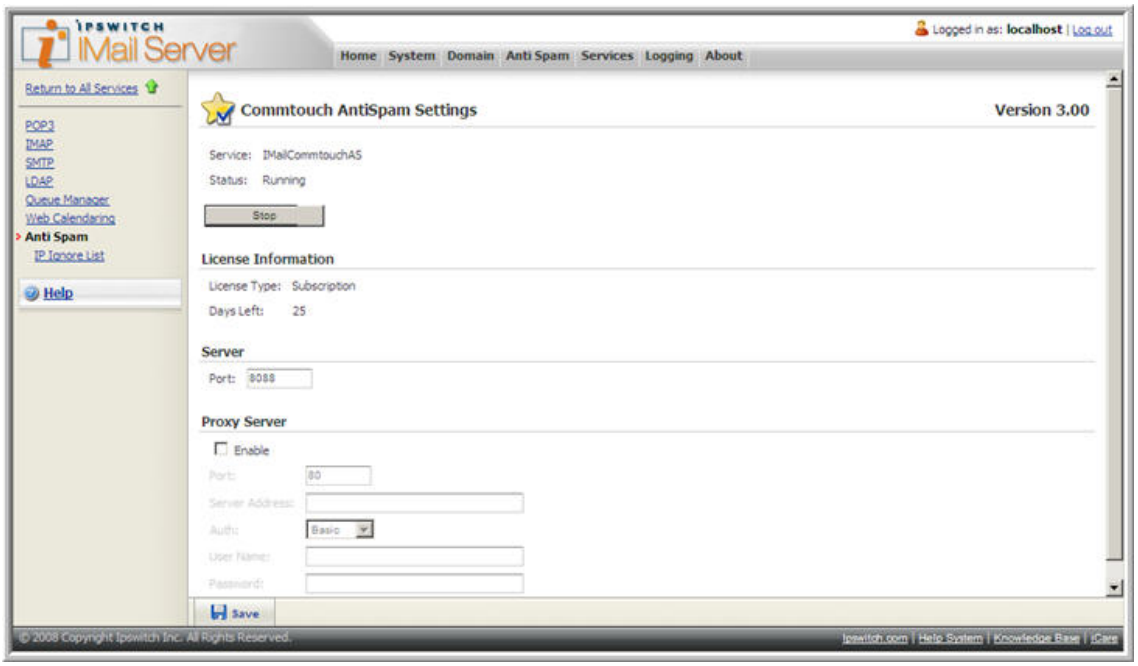
After installing you can access the Antispam settings by clicking the **Antispam** tab in IMail Administrator. The **Domain Level Spam Filter** page appears.



To access the Premium Antispam settings(available only with IMail Plus and Premium), click the **Premium Filter** link.



To access Premium Antispam Service settings go to **Services** > **Antispam.**



What You Can Do with the Antispam Features

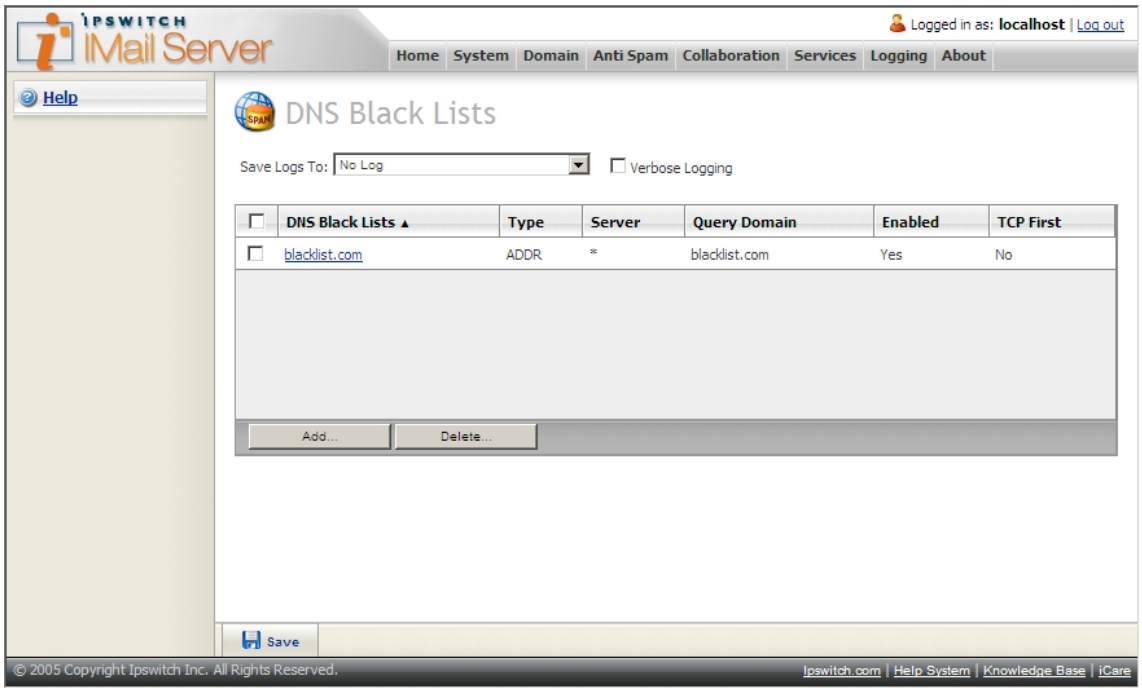
- Create a **White List** (trusted addresses) of e-mail addresses, domains, and subnet masks that bypass content filtering.
- Use **Connection Filtering** to compare e-mail messages against configurable DNS black lists to determine if they are from IP addresses that are known to send spam.
- Enable verification checks (connection filtering) to verify the "Mail FROM" address, HELO/EHLO domain information, and perform a reverse DNS lookup on incoming e-mail messages.
- Use the **Sender Policy Framework** (SPF) feature to increase the ability to stop incoming e-mail from forged e-mail addresses (spoofed e-mail).
- Use the **Premium Antispam** filter (available with IMail Plus and IMail Premium only) to automatically manage spam protection with Commtouch Advanced Security Daemon (ctasd™) antispam technology. Premium Antispam filter settings are applied to incoming mail before Standard Antispam filter settings.
- Use **Phrase Filtering** (content filtering) to configure a phrase list that searches for specific spam phrases within the subject and body of e-mail messages.
- Enable **Statistical Filtering** (content filtering) to analyze each message and determine if it is spam.
- Enable **HTML Feature Filtering** to search messages for HTML tags that could be used to disguise spam.
- Create a **URL Domain Black List** that searches for domain names (URLs) contained within HREF and IMG SRC HTML tags and in plain text messages.

- Enable **Broken MIME Header** filtering to treat e-mails with malformed MIME headers as spam.
- Configure delivery **Rules** to trap messages based on spam X-Headers that are inserted when a mail message fails a spam test.

Accessing the Antispam Features

The Antispam options are accessed from two levels; the server level and domain level:

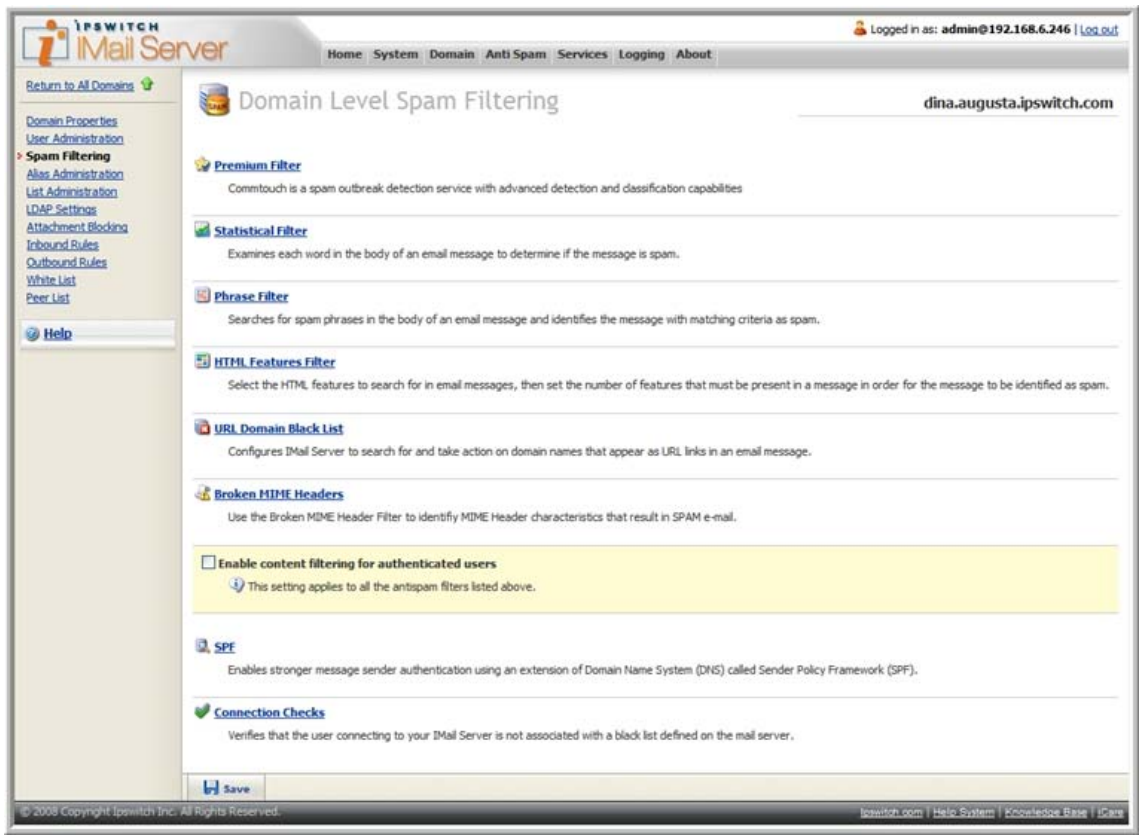
- **Server level settings**. Mouse over the IMail Administrator **System** tab, then click **DNS Black Lists**. The DNS Black Lists page opens.



Use this page to configure and enable all black lists at the server level. All black lists must be configured and enabled at the server level before an IMail e-mail domain can use them. This lets a system administrator decide which black lists to allow an e-mail domain to use. Only black lists that are enabled on the DNS Black Lists page are available for use in domain (host) level configurations.

Use DNS Black Lists Options to add, edit and delete server black lists. All black lists that are currently configured for the server are displayed in the DNS black list.For more information, see the **IMail Administrator Help**.

- **Domain level settings**. Click the IMail Administrator **Antispam** tab. The Antispam Settings page opens.



Use the Domain Level Antispam settings to enable, change, and disable various antispam filters for the selected domain:

- **Premium Filter** (available only with IMail Premium and IMail Plus). Provides fully automated spam protection in addition to the standard antispam filter included in IMail Server. For more information, see "Forwarding Spam to Ipswitch" on page 40.
- **Statistical Filter**. Examines each word in the body of an e-mail message to determine if the e-mail is spam.
- **Phrase Filter**. Searches for spam phrases within the body of e-mail messages and identifies the messages that are spam.
- **HTML Features Filter**. Searches HTML features in messages that are subject to spam. Sets how many HTML features must be present in an .htm file in order for a message to be identified as spam and the spam action to take.

- **URL Domain Black List**. Searches for domain names that appear as URL links in messages, and lets you set the action to take on such messages.
- **Broken MIME Headers**. Uses the Broken MIME Header Filter to identify MIME Header characteristics that result in SPAM e-mail.
- **Enable content filtering for authenticated users**. Select this option to enable content filtering for all messages that are received from authenticated users.

Note: Even if the **Enable content filtering for authenticated users** option is selected, content filtering is not performed on messages that are sent from system and host administrators. This prevents mail from being filtered twice in cases where a message is mis-identified as spam and the administrator then forwards it on to its intended recipient.

- **SPF (Sender Policy Framework)**. Enables stronger authentication of e-mail senders using Sender Policy Framework (an extension to the DNS system). Provides administrators increased capability to stop incoming e-mail from forged (spoofed) e-mail addresses.
- **Connection Checks**. Verifies that the party connecting to your server is not part of a black list.

  For more information, see the **IMail Administrator Help**.

Forwarding Spam to Ipswitch

The Premium Spam Filter performance can be improved when users forward spam e-mail to Ipswitch. Ipswitch provides the spam mail to Commtouch Advanced Security Daemon (ctasd™) editors to review the spam submission and add spam signature information to it. Then the signature is published to the global database to help other users eliminate spam. For maximum protection, this global database is updated on your IMail Server every few minutes.

To forward spam e-mail to Ipswitch:

- If you receive a spam message in your mailbox, forward the e-mail to **reportspam@ipswitch.com** (mailto:reportspam@ipswitch.com).

  The Premium Spam Filter focuses on eliminating false positive e-mail. However, if you receive a false positive message, forward the e-mail so it can be added to the global database to assist in eliminating future spam.

To forward false positive spam e-mail to Ipswitch:

- If you receive a false positive spam message in your mailbox, forward the e-mail to **falsespam@ipswitch.com** (mailto:falsespam@ipswitch.com).

CHAPTER 7

Mail Servers and the DNS

In This Chapter

What is DNS? 45

How a Mail Server Uses DNS 46

Setting Up Mail Server Records in the DNS 47

What is DNS?

DNS (Domain Name Service) is the mechanism by which a program running on your host computer can locate the address of other hosts on the Internet, and by which other hosts on the Internet can locate you. The DNS essentially provides a map of the structure of the Internet.

Organizations must register a domain name with the InterNIC and obtain addresses to use for the hosts in their domain. For example, ipswitch.com is a registered domain name, and some addresses assigned to ipswitch.com are 156.21.50.1 through 156.21.50.255. For information about registering a domain name, see the InterNIC's Web site at **http://www.internic.net**.

All hosts on the Internet must have a host name and an IP (Internet Protocol) address. You can give a host any host name you want, as long as it is unique within your domain. For example, some host names and addresses in the ipswitch.com network are:

```
test1.ipswitch.com  156.21.50.1

test2.ipswitch.com  156.21.50.2

test3.ipswitch.com  156.21.50.3
```

DNS servers provide the mapping of host names to their addresses. The DNS server for ipswitch.com lists each Ipswitch host and its corresponding address. Thus, any host outside of ipswitch.com can query the DNS server for ipswitch.com to find the address of a particular host. Once it has the address, the requesting application can communicate directly with the host. Note that querying a DNS server is also called a "DNS lookup" or a "lookup."

When a host outside ipswitch.com wants to send mail to a user on the ipswitch.com network, it queries the DNS server for ipswitch.com to find the mail server for users on ipswitch.com. The host can then send mail to the mail server, which will deliver it to the appropriate user.

How a Mail Server Uses DNS

All SMTP mail servers that communicate with other Internet hosts use a DNS server to look up mail addresses. The basic communications between a mail server and a DNS server work as follows for incoming mail and outgoing mail.

Incoming Mail:

To illustrate how a DNS server is used to look up mail addresses, we use the example of what happens when a user on another Internet host sends mail to a user on your IMail Server host (for example to fred@domain.com).

1. A user sends mail to your user, fred@domain.com.
2. The sending mail server asks the DNS server on the domain.com network for the host name of the mail server. The MX (Mail eXchanger) record in DNS identifies the Host Name of the mail server.
3. The DNS server for domain.com returns the value of the MX record, which is the host name of the mail server, in this case, mail.domain.com.
4. The sending mail server now asks the DNS server on the *domain.com* network for the address of the mail server host (mail.domain.com). The A record in DNS maps the host name to an IP address.
5. The DNS server for domain.com returns the value of the A record for the mail server host (mail.domain.com), which is the IP address (156.50.1.5).
6. The sending mail server connects to the receiving mail server's IP address and sends the mail.

Outgoing Mail:

When one of your IMail Server users sends mail to a user on another Internet host (for example, to sam@widgets.com), the same process occurs, except that it is your mail server that does the lookups for MX and A records on the DNS server for the widgets.com network.

Reverse Lookups

Note that some mail servers, upon receiving mail, will do a "reverse lookup" on the address to make sure it is valid. This is done in an attempt to thwart bulk mailers who may be illegally using someone else's mail server to relay mail. A PTR record attempts to verify that the inbound e-mail is originating from a mail server and not a workstation. To do a reverse lookup, the receiving mail server asks the DNS server on the sending mail server's network to confirm that the IP address of the sending server matches the host name of the sending server.

Reverse lookups are enabled in DNS by creating a PTR record for the mail host. The PTR record maps an IP address to a host name.

Setting Up Mail Server Records in the DNS

To set up your mail server in the DNS, you must create the records that other mail servers use to find and connect to your mail server. Making these entries requires that you first have:

- A registered Internet domain name for your local network (for example, domain.com).
- A DNS server for your local network.

Configuring Your Local Network DNS server

Before your mail server can communicate with other mail hosts, you must configure the DNS server to recognize your mail server. Without a functional and correctly set DNS, IMail Server cannot deliver mail, except to domains that are within IMail Server.

For each mail host on your network, you must make the following entries in your DNS:

- An MX record for the mail domain (for example, domain.com). The MX record identifies the host name of the mail host. Note that mail hosts (virtual hosts) that do not have an IP address require only an MX record.
- An A record for the host name of the mail host. The A record maps a host name to an IP address.
- A PTR record for the IP address of the mail host. The PTR record maps an IP address to the host name and is used for reverse lookups.
- An SPF record lets other e-mail servers use SPF filtering (if the feature is available on the mail server) to protect against incoming e-mail from forged (spoofed) e-mail addresses that may be associated with your mail server. As SPF records are implemented more widely, SPF filtering will become more effective at identifying spoofed e-mail messages. For more information about SPF records, see the *IMail Administrator Help*.

Since there are DNS servers from many vendors available, we cannot describe how to create the records for your specific DNS server. Instead, we show an example using a basic configuration for a single mail host.

Example of a Basic Configuration

In this example, we use a DNS lookup tool to query the DNS server and show the responses. You can use the Windows NT command line program, NSLOOKUP, to query a DNS server. If you are not familiar with this tool, we suggest the Ipswitch WS_Ping ProPack application, available as a demo at *http://www.ipswitch.com/_download/main.asp?product=WP-0000* http://www.ipswitch.com/_download/main.asp?product=WP-0000, which provides a graphical interface for querying a DNS server. Use the Lookup tool in WS_Ping ProPack.

To describe the DNS entries for a mail server, we use examples from a typical small network and start with the following assumptions:

- You have one computer with a network interface card (NIC) installed.
- You have set the IP address for this computer to a valid address within your range of addresses. In the example, we will use 156.21.50.5.
- You have assigned this computer a host name that is valid in your domain. In the example, we will use mail.domain.com.

- You have designated another SMTP server to act as a backup if your mail server is down. In the example, we will use cecil.domain.com.

You must set up the following records for the computer:

- An MX record for the domain **domain.com** that points to the host name of the computer running IMail (**mail.domain.com**).
- An A record for mail.domain.com
- A PTR record for mail.domain.com

E-mail for the users on this mail host is addressed to user@domain.com.

First, we do an MX lookup (just as a sending mail server would do) to find the mail host for the domain.com network. To simulate this, in the WS_Ping ProPack's Lookup tool, we enter **domain.com** in the Name/Address box and **MX** as the Query Type, which returns the following:

```
domain.com
```

This shows that mail.domain.com and cecil.domain.com are both mail hosts for the domain.com network. The cecil.domain.com host is a backup mail server. The number indicates the priority of the mail host — it tells the sending mail server which mail host to try first. The lower the number, the higher the priority. In our case, mail.domain.com is the one we want other mail servers to use first; cecil.domain.com is used only if mail.domain.com is down.

For information about how a backup mail server works, see "Setting Up IMail Server as a Backup Mail Spooler" in the **IMail Administrator Help**.

Only a host name is returned in response to an MX query. The sending mail server needs the IP address of this host name so it can connect to the mail host. The sending mail server performs another DNS lookup to get the IP address (defined in the A record) of highest priority mail host. To simulate this, in the Lookup tool, we enter mail.domain.com in the **Name/Address** box and A as the Query Type, which returns the following:

```
mail.domain.com
```

If we query the A record for cecil.domain.com, we get:

```
cecil.domain.com
```

With the IP address for the mail.domain.com host, the sending mail server can now connect to that host and deliver the mail. If the attempt is successful, there is no need to go any further. However, if the mail.domain.com host is down, the connection attempt fails and the sending mail server will have to try the next highest priority MX record, in this case, cecil.domain.com.

Sample DNS Records

If we use a DNS lookup tool to query the DNS server for the network in our example (for all information, in verbose mode), you would see entries like the following:

```
domain.com.  IN MX   50 cecil.domain.com.

 IN MX   10 mail.domain.com


cecil.domain.com.  IN A  156.21.50.100

mail.domain.com.   IN A  156.21.50.5


5.50.21.156.in-addr.arpa.,type = PTR

 host = mail.domain.com

5.100.21.156.in-addr.arpa.,type = PTR

 host = cecil.domain.com
```

Other Configurations

If you have multiple mail hosts on your IMail Server, you will need an MX, A, and PTR record for each host. For more information, see "*Setting Up DNS for Multiple Mail Hosts* (on page 8)".

Index

A

A record 8, 46
  verifying 25
adding users 30
Alias 27
antispam
  administration
    domain level 42
    server level 42
  filtering types 41
antispam features
  reinstalling 34
antispam-table.txt
  antivirus administration
    IMail Administrator 35
    Symantec Administrator 35
  ignoring file modification 34
  merging new file 34
  overwriting current file 34
authentication
  SMTP 14

C

client
  browser application 30

D

Data Source Name. See System DSN 10
database
  confirming setup 28
  external 10
  IMail 10
  selecting 17
database, users 10, 28
DNS
  and mail servers 45
  description 45
  entries
    A records 7
    background information 8
    confirming 25
    mail server 6
    MX records 7
    PTR records 7
    SPF records 7
  how it works 46
  lookup 45
  multiple hosts 8
DNS Black List 42
DNS server 2
domain name 6
domains
  single or multiple 14

E

email
  services 11
email clients
  application 2
  browser-based 2

F

forum 3

H

help resources 1
host alias 27
hosts
  multiple 14
  primary 6
  virtual 8

I

IMail client
  console application 30
IMail Server
  selecting user database 10
  testing
    database 28
    DNS settings 25
    mail account 30
    server 27

uninstalling 34
IMail Server Administrator
starting 27
IMail Web Messaging
starting 30
installation 15
planning 5
testing 23
IP address 6
for virtual host 8
Ipswitch Web site 2

L

lookup
query DNS server 45
lookup tool
nslookup 25
WS_Ping ProPack 25

M

mail domains
virtual 8
mail server
DNS entries 6
installing 15
security 12
services 11
testing 23
mail services
selecting 17, 19
mail system
components 2
MX record
defined 8
verifying 25

O

ODBC database 10

P

PTR record 8, 46
verifying 25

R

relay options 13
release notes 1
reverse lookup 8, 46

S

security
mail server 12
SMTP authentication 14
SSL keys 18
services
email 11
selecting 19
SMTP authentication 14
spam
forwarding to Mail-Filters 42
SSL keys 18
System DSN 10

T

testing
send and receive mail 30

U

uninstalling
IMail Server 34
upgrading
antispam features 34
IMail Server 32
user database
confirming setup 28
user forum 3

V

virtual hosts
with IP addresses 8
without IP addresses 8

W

Web Messaging
starting 30
Windows NT registry 34
Windows user database 10