



SpamLion, Inc.

Sender Validation Gateway™

Sender Validation Gateway™

Installation Guide

Version 1.80.95

Sender Validation Gateway™ - Installation Guide v1.80.95

To Our Customers

Thank you for purchasing SpamLion's Sender Validation Gateway, the most effective anti-spam solution ever made. You will soon experience an unprecedented level of protection - without losing your real email. Please use this guide and the technical expertise of our experienced resellers to ensure a trouble-free installation.

Copyright © 2002-2006 by SpamLion, Inc.

All rights reserved. This document is intended for the sole use of the purchaser of the Sender Validation Gateway™ software, hereafter referred to as the *Gateway*. No part of this document may be reproduced, stored in a retrieval system or distributed by any means electronic, mechanical, photocopying, recording, or otherwise without written permission from the publisher.

Trademarks

This document may contain references to trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of SpamLion, Inc. or such third parties.

Warning and Disclaimer

No liability is assumed with respect to the use of the information contained herein. Although precautions have been taken in the preparation of this document, SpamLion, Inc. assumes no responsibility for errors or omissions. No warranty or fitness is implied. The information provided is on an "as is" basis. SpamLion, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising for the information contained herein. Neither is any liability assumed for damages resulting from the use of the Gateway.

Tell Us What You Think

As the reader of this publication, you are our most important critic and commentator. Please send comments and corrections to: support@spamlion.com



Tips provide information to make installation easier.



Knowledgebase articles provide additional information.



Warnings help avoid common installation issues.

SpamLion, Inc.
P.O. Box 549
Cotati, CA 94931
(800) 761-SPAM
www.SpamLion.com

Table of Contents

INTRODUCTION	1
REQUIREMENTS	1
PLACEMENT	2
MESSAGE FLOW	2
SUPPORT	4
PREPARATION	5
NETWORK DISCOVERY AND PLANNING	5
CONFIGURATION WORKSHEET	7
PREPARING YOUR SERVER	9
GATEWAY SOFTWARE AND LICENSE FILE	10
LOCATE THE SPAMLION.LIC LICENSE FILE	10
INSTALLATION	11
1. INSTALL GATEWAY SOFTWARE	11
2. TEST AND CUTOVER OUTGOING EMAIL	12
3. SETUP AND TEST INBOUND HTTP	14
4. TEST AND CUTOVER INBOUND EMAIL	14
ADDITIONAL INSTALLATION FEATURES	15
1. SYNCHRONIZE RECEIVERS' EMAIL ADDRESSES – MICROSOFT EXCHANGE	15
2. SYNCHRONIZE RECEIVERS' EMAIL ADDRESSES – OTHER EMAIL SERVERS	16
3. ENABLE DICTIONARY ATTACK DEFENSE	17
4. CUSTOMIZE THE WELCOME NOTICE (VALIDATION/REGISTRATION NOTICE)	17
5. AUTOMATED AND MANUAL WHITELISTING	18
6. CONFIGURE SMTP EMAIL DELIVERY SETTINGS	20
7. DEFINING ADDITIONAL DOMAINS	20
DEPLOYMENT	21
MAINTENANCE	23
LICENSING	24
UNINSTALL	25
APPENDIX I (IIS 5.0)	29
APPENDIX II (IIS 6.0)	32

Introduction

This guide describes placement and installation practices for the Sender Validation Gateway™. We highly recommend reading this guide in its entirety, prior to installing this product. Additional knowledge base articles may be required for your specific network environment.

Instructions for configuration and network administration of the installation computer, firewall and protected email server are not specifically detailed in this document and will require a qualified network engineer with a working knowledge of your network and these other systems.

Requirements

Hardware

The efficiency of *Sender Validation* eliminates the need for a high-powered system.

Minimum (less than 1,000 users, or less than 1M emails a month):

- Pentium III, 800Mhz
- 128MB RAM, 20GB HDD (Win. 2000 Server)

Recommended (thousands of users, or millions of emails a month):

- Pentium 4, 2.4Ghz
- 256MB RAM, 80GB RAID (Win. 2003 Server)

Operating System

Microsoft Corporation recommends:

- Windows 2000 Server
- Windows Server 2003
- Windows Virtual Server 2005

Some small businesses have successfully used:

- Windows 2000 Professional
- Windows XP

Web and SMTP Services

Microsoft's Internet Information Services must be configured as show in Appendix I or II to reliably provide web and email transport processing for the Gateway.

- IIS 5.0 – Appendix I
- IIS 6.0 – Appendix II

Protected Email Server Requirements

The Gateway will protect any Internet compatible email server, thereby protecting its users. *For limited deployments, the Administrator can select which users are protected.*

- Exchange 5.5
- Exchange 2000
- Exchange 2003
- GroupWise
- Lotus Notes
- UNIX (Sun, AT&T, HP, etc.)
- Linux
- Apple
- All Internet compliant PO's.

Sender Validation™ Requirements

The Sender Validation detection process supports all sources of email, including those listed above, plus cell phone and PDA based email. Additionally, one-time *manual validation* is available, should an unknown source not support bidirectional communication.

Placement

The Gateway is typically placed between the Internet and your email server(s), behind your company's firewall.

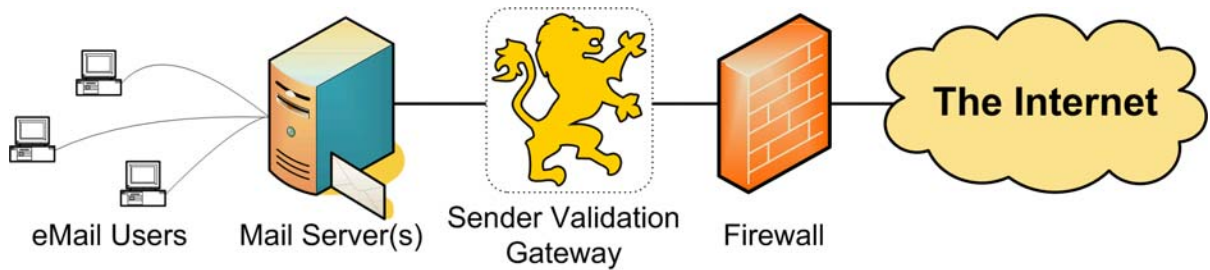


Figure 1, Gateway placement



Anti-Virus Systems are placed between the Gateway and the Mail Server, or better yet, **installed on the mail server** to protect the proliferation of intra-office viruses. If you must install it on the Gateway, first *contact the anti-virus manufacturer to ensure you know how to configure their software to **not interfere** with IIS's Web and SMTP services or the Gateway's files or processes.*

Message Flow

Outbound Auto-Validation

This feature enables the Gateway to selectively learn who your company communicates with by analyzing outbound email from your email server(s). These people (and entities, such as requested newsletters) are auto-whitelisted to eliminate false-positives.

Your email server (or anti-virus system) will be set to deliver outbound email to the Gateway.

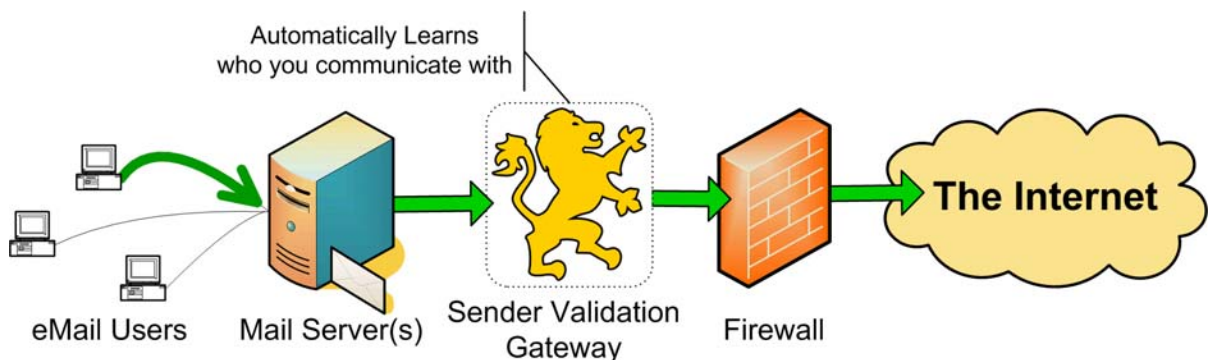


Figure 2, Outbound Auto-Validation

Message Flow (Continued)

Inbound Protection

The Gateway passes email from **all valid sources** on to your *Protected Post Office* (email server), while holding email from **questionable sources** in its internal Quarantine – until a one-time validation occurs (either automatically or manually).

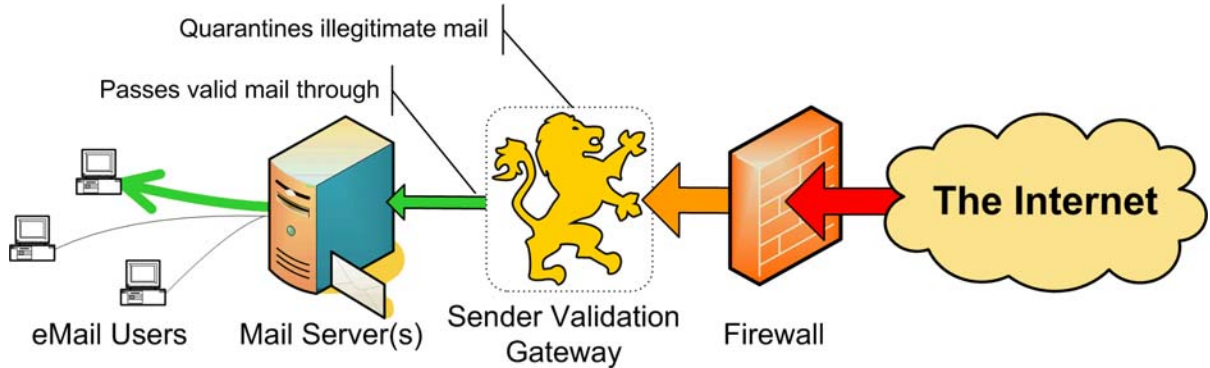


Figure 3, Inbound Protection



Each person will have access to their *own browser-based Quarantine Manager*, enabling them to perform a one-time manual validation for any new automated source, such as an e-commerce receipt from a new vendor. Please see our Demo Videos.

First Contact Analysis and Validation

Emails from unidentified sources are known as *First Contact¹* messages. The Gateway will automatically send them your customized “Welcome Notice” (Registration/Validation Notice) with an imbedded “Opt-In Validation™” URL, enabling real people to be instantly validated.

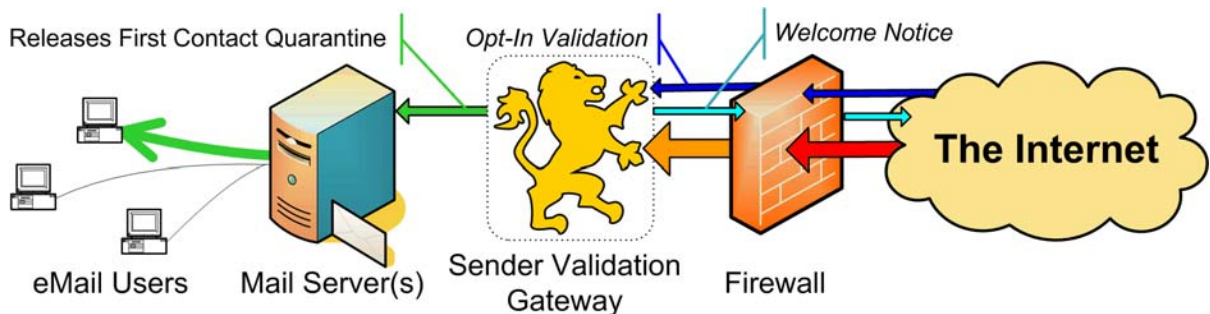


Figure 4, First Contact Validation



The **simple Opt-In Validation™** is easy for real people to use – just one click. However, for spammers, it's nearly impossible: in over three years, and stopping over a billion spams, not a single automated spammer has ever Opt-In Validated.

¹ Please review our *Whitepaper on First Contact Analysis* to learn about this new discovery, and its ability to isolate spam with 100% accuracy while not interfering with any real email.

For the latest support information, including *instructional videos*, please visit:

<http://www.SpamLion.com/Support>

Minimizing Support Headaches

Contacting the appropriate vendor is better than aspirin. First determine the source of the problem: the operating system (Windows), your network, firewall, DNS, email server, Internet connection, or other software (that interferes with IIS's web or SMTP services).



Please contact your network systems experts or the appropriate manufacturer first.

Requesting our staff to verify that the Gateway is running properly is a billable service, and generally will not resolve the actual cause of the problem.

Sender Validation Gateway™ Product Support

Our product is priced so that training, troubleshooting, and other support is only charged to those who specifically request them in lieu of using documentation, training videos, our knowledge base, or using their own networking experts.



Even paid support can not substitute contacting the appropriate manufacturer or finding an experienced network systems consultant, as our staff only assists with the configuration and use of the Gateway itself.

First Line Support

First ask the SpamLion Reseller or Partner you purchased the product from for assistance – most have experience assisting with network planning and troubleshooting, as well as with the Gateway.

SpamLion Paid Installation Assistance

Optionally, our staff can assist with planning, live installation, and training using remote control (PCAnywhere, NetMeeting, GoToMyPC, WebEx, VNC, etc.). To utilize our services affectively, you will need to have a properly configured server, someone who knows how to configure your firewall (as specified in this document) and someone capable of independently troubleshooting your network.

Currently² installation assistance (limited to two hours) is included for **free with purchases of over 200 users**. For all smaller purchases, please inquire about current rates.

To open a support ticket, visit <http://www.SpamLion.com/SupportRequest> or call our corporate office at 800-761-SPAM and have a customer service representative open a ticket for you.

Support hours are M-F, 8am-5pm Pacific Time, excluding holidays.

¹ Please check with SpamLion, Inc. before purchasing the product for current installation and support offerings.

Preparation

The first step in the planning process is to review exactly how email flows between your business and the Internet. Then determine the appropriate changes to route incoming and outgoing email through the Gateway. Next, determine how you'll expose the Gateway's HTTP Validation interface. And finally, make sure the necessary people know how to perform and test these changes, in real-time on your live network.



Please do not substitute the Gateway's simple installation process for proper planning. Although these steps **ensure no interruption of live mail flow** (even when a problem occurs), proper planning ensures first time success.

Network Discovery and Planning

Exchange Servers (5.5, 2000, and 2003)

Please familiarize yourself with the **Smart Host** setting, as you will need to set this to have Exchange forward all Outbound email to the Gateway. You will be setting it to the Gateway's IP address.



KB200509-3 depicts this setting for all three versions of Exchange.

Other Email Servers

Most all email servers have a setting to forward all **Outbound** email to another host, gateway, relay, remote, or other such device. If you are unable to locate this setting, please contact the appropriate manufacturer to discover how to configure their email server.

Firewall

First, find the firewall rule that **forwards Inbound SMTP** (port 25) traffic to your email server, as you will be altering this rule to send email to the Gateway.



If you have **Remote Offices** or **Remote Users**, please seek the guidance of an experienced SMTP Routing Architect, to design an appropriate message flow path for your unique situation. Usually all that's needed are simple firewall rules, SMTP restrictions, or a VPN (included with Windows for free).

Second, the Gateway includes a built-in website to process the unique *One-Click-Validation*TM in each First Contact *Welcome Notice*³. To expose this website to the Internet, you need to create an **Inbound Rule for HTTP** (port 80 or other).

³ The Welcome Notice is also known as a Registration Request or a Validation Notice.

Firewall (continued)



If using an **alternate port**, and you prefer not to configure your firewall to translate that port back to port 80, please add the alternate port to IIS using the information in **KB-200509-2**.



If you have **only one IP address for Internet access**, and port 80 is already in use for another website or browser-based email (such as Exchange Server's Outlook Web Access – OWA), you will need to use another port, such as 8080, 8088, etc. Contact an experienced firewall/network consultant if help is needed.

Outside URL

Once you know how the Firewall will be configured, you can choose the format of the One-Click Validation™ URL that will be in each Welcome Notice. This “Outside URL” should have a FQDN (fully qualified domain name) in DNS, with an alternate port number, if needed. Alternatively you can use an IP address.



Studies have shown **people respond best** to a Welcome Notice with a URL that is your domain name rather than an IP address. We recommend creating a DNS entry such as sl.[your domain name].

Inside URL

The second URL is used to access the Quarantine Manager (Inside URL). It can also have an FQDN or an IP address, and may or may not require an alternate port see KB200509-2 on alternate port configuration.

Typical installation:

Welcome Notice (Outside) URL = `http://sl.spamlion.biz`

Quarantine Manager (Inside) URL = `http://10.1.1.57`

or, if no FQDN exists for the Outside:

Welcome Notice (Outside) URL = `http://64.166.129.248/`

or, if using an alternative port, such as 8080 on the outside:

Welcome Notice (Outside) URL = `http://sl.spamlion.biz:8080`



Experienced Gateway installers have helped many businesses with very unique networks. If an easy solution isn't obvious, contact our support group for a free suggestion or a referral to an experienced installer that offers consulting services.

Configuration Worksheet

The following information will be needed during your Gateway installation. To save time and frustration, please record them on this worksheet prior to starting the actual installation.

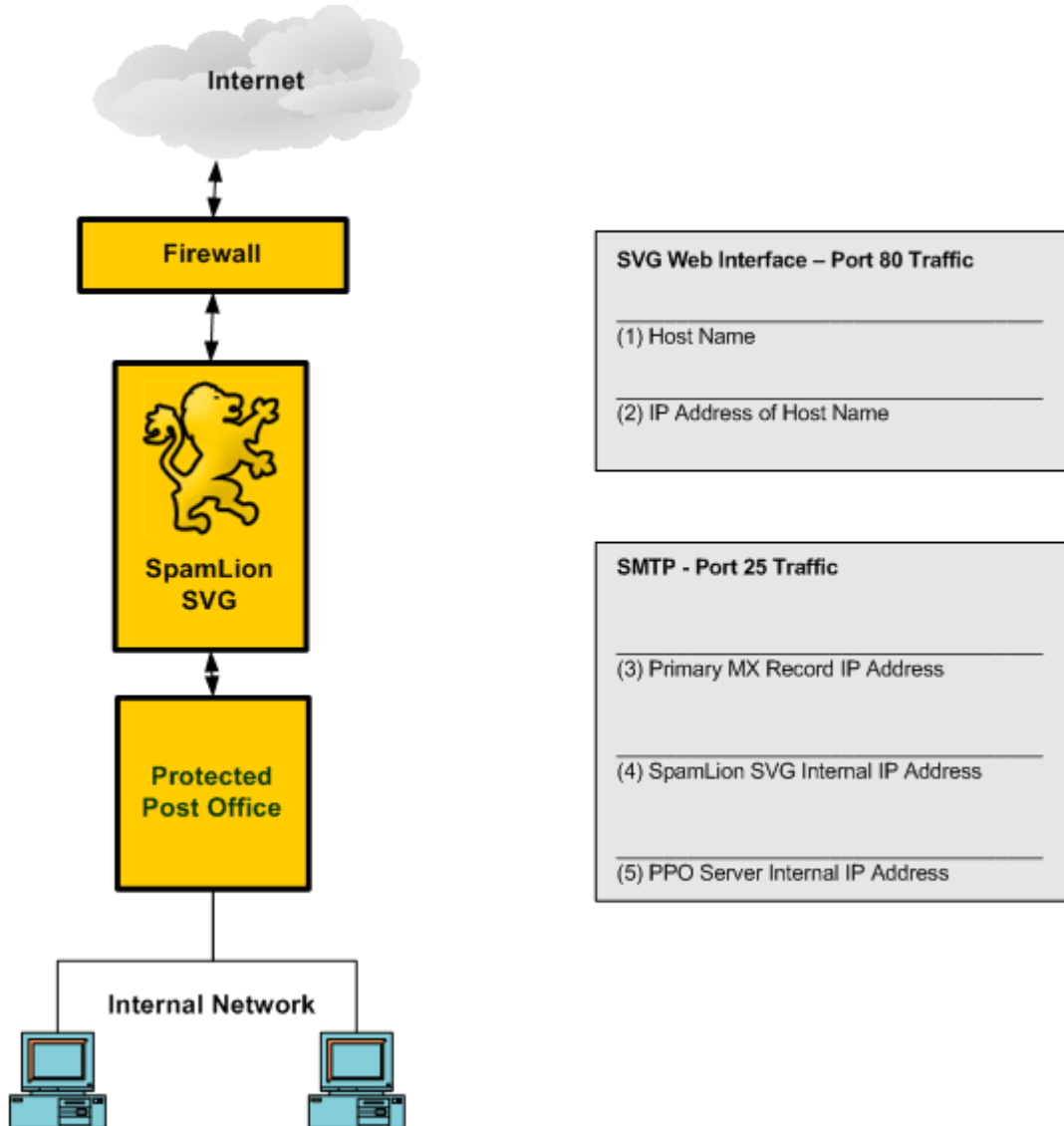


Figure 5, Configuration Worksheet

SVC Web Interface – Port 80 Traffic

(1) Host Name

The fully qualified domain name, or Host (A Record) listed on your DNS server, that will correspond to the Internet accessible IP address for port 80 traffic to the Gateway.

Example: s1.epubz.com

Used to configure your DNS server to enable the “Outside URL”, which will appear in the Welcome Letter. It facilitates First Contact self-validation via the Gateway’s web interface.

(2) IP Address of Host Name

The external IP address defined in DNS for the Outside URL discussed in (1) Host Name.

Example: 72.245.23.78

It is used to configure your firewall to route port 80 (HTTP/HTTPS/WWW) packets from this address to the Gateway's internal address (4).

Example Firewall Rule (Cisco PIX) – See Installation Video for Kerio Firewall example:

```
static (inside,outside) 72.245.23.78 10.0.0.3 netmask 255.255.255.255 0 0
conduit permit tcp host 72.245.23.78 eq www any
```

SMTP – Port 25 Traffic

(3) Primary MX Record IP Address

The existing MX record in DNS that directs incoming mail to your firewall.

Example: 72.245.23.78

Used to locate which Firewall MX (SMTP) Rule will be reconfigured.

DNS example for epubz.com:

```
@           MX 10      mail.epubz.com.
mail        A          72.245.23.78
```

Example of a *pre-existing* Firewall Rule (Cisco PIX) - See video for Kerio example:

```
static (inside,outside) 72.245.23.78 10.0.0.2 netmask 255.255.255.255 0 0
conduit permit tcp host 72.245.23.78 eq smtp any
```

(4) SpamLion SVG Internal IP Address

The IP address assigned to the NIC on the server running the Gateway software.

Example: 10.0.0.3

This address will be used when reconfiguring the Firewall's SMTP traffic.

Example Firewall Rule (Cisco PIX) – See Installation Video for Kerio Firewall example:

```
static (inside,outside) 72.245.23.78 10.0.0.3 netmask 255.255.255.255 0 0
conduit permit tcp host 72.245.23.78 eq smtp any
```

(5) PPO Server Internal IP Address

The IP address assigned to the NIC on the Protected Post Office (PPO or mail server).

Example: 10.0.0.2

Used when configuring the Gateway to pass non-spam mail on to the staffs' mail server.

See Figure 6, *Gateway Installation Settings*.

Preparing your Server

Select a computer system that meets the criteria previously described in “Requirements.”

Before customizing a server with your preferred software and settings, please start with a newly installed (or reinstalled) fully working “clean” system: just the base O.S. with IIS, per our specification.



To **avoid installation difficulty and reliability issues**, please do NOT install any other software, use any “lock-down” tools, or customize the IIS settings, unless you fully understand how to prevent their conflicts with IIS’s services and the Gateway.



If you want to join a domain, please do so *after* the Gateway is installed and properly functioning. Otherwise you will need to **manually grant** IIS’s Web Services (the IUSR_[machine name] account) with **Modify** access to SpamLion1 and all sub-folders.

Windows 2000 Server, Professional and XP

Carefully install Internet Information Server 5.0 (IIS) with ONLY: Common Files, IIS Manager SnapIn, SMTP Service and World Wide Web Service.



Use **Appendix I** as a quick step-by-step guide to ensure proper IIS setup.



Microsoft advises against using **Professional and XP**, as they are not designed to be “servers”. It appears the only limitation is 10 simultaneous SMTP sessions, which may work fine in low-traffic situations. Most small businesses that use these O.S.’s report no problems, but a few have reported extreme difficulty (even with Microsoft helping them).

Windows Server 2003 (all Editions)

Carefully install Internet Information Server 6.0 (IIS) with ONLY: Common Files, IIS Manager SnapIn, SMTP Service and World Wide Web Service.



Use **Appendix II** as a quick step-by-step guide to ensure proper IIS setup.

Gateway Software and License File

Use the CD-ROM or download the most current software from the SpamLion FTP site:

<ftp://ftp.spamlion.com/download>.

Navigate to the **Installation-Gateway-v1.80** folder.

You can run the self-extracting archive file directly from the FTP site, or you can download the EXE or ZIP file to your hard disk and extract from there.

The installation archive contains only one file, Setup.exe, which we recommend placing on your desktop during installation.

Place this file in a safe place in the event you need to:

- Install the Gateway on another computer and recover from a backup
- Uninstall the Gateway (by running Setup and selecting *Remove*)

Locate the SpamLion.lic license file

Place the product's license file, "spamlion.lic", on to your Desktop.

The license file should be an attachment to an email message sent to you by SpamLion, Inc. or from your Authorized Partner or Reseller.



Remember, the license file enables the product to protect a limited number of users for your Mail Domain (DNS's MX records). If your company uses more than one domain name for email, you will need to obtain a license that covers all the domains you want protected by the Gateway. Domain additions to the license file are free during the initial purchase, but inquire about license restrictions.

Installation

Having planned the installation, and being ready to make email Server and firewall changes, you are now prepared to install and test the Gateway in a live environment.



Although this process ensures proper installation without disrupting live email flow, it is strongly recommended an experienced Gateway installer be present (in person or remotely), because if any step or test result is unclear, you should not continue until the potential problem has been resolved.

1. Install Gateway Software

1. Doubleclick to launch Setup.exe (from the desktop, CD-ROM, etc.).
2. Accept the License agreement to continue.
3. Verify and complete the Installation Settings form (*figure 6 on the next page*):
 - a. Verify your **License Information**
 - Does it protect the correct number of mailboxes?
 - Is your company's name spelt correctly?
 - Are all your domain names spelt correctly?



*If there are any errors with the License Information, **cancel** the installation, and obtain a corrected license file through your reseller or SpamLion, Inc.*

- b. Select the **Installation Destination** (typically Drive C)
 - c. Is **This computer's Server IP Address** correct? (if not, cancel the installation, change this computer's IP address, and restart the installation).
 - d. Review the **Quarantine Notice's URL**, and ensure it matches with your plan.
 - e. Review the **Quarantine Notice's From email Addresses**, typically this your company's Help Desk or email administrator. This is only used for internal notices.
 - f. Review the **Validation Notice's URL**, and change it if during planning you decided not to use the FQDN shown by default. Do you need to specify an alternate port?
 - g. Fill in **your email Server's IP Addresses**
 - h. Provide an **email Address for the Administrator Logon**. The system uses this to notify you of any problems so it should be your email address.
4. Note the default Username and Password. Once the installation is complete, you should change the password and record them somewhere safe. If lost, open a support ticket, and send a copy of the database to SpamLion, Inc. for recovery.
 5. Press **Install**, to complete the installation.

Install Gateway Software (continued)

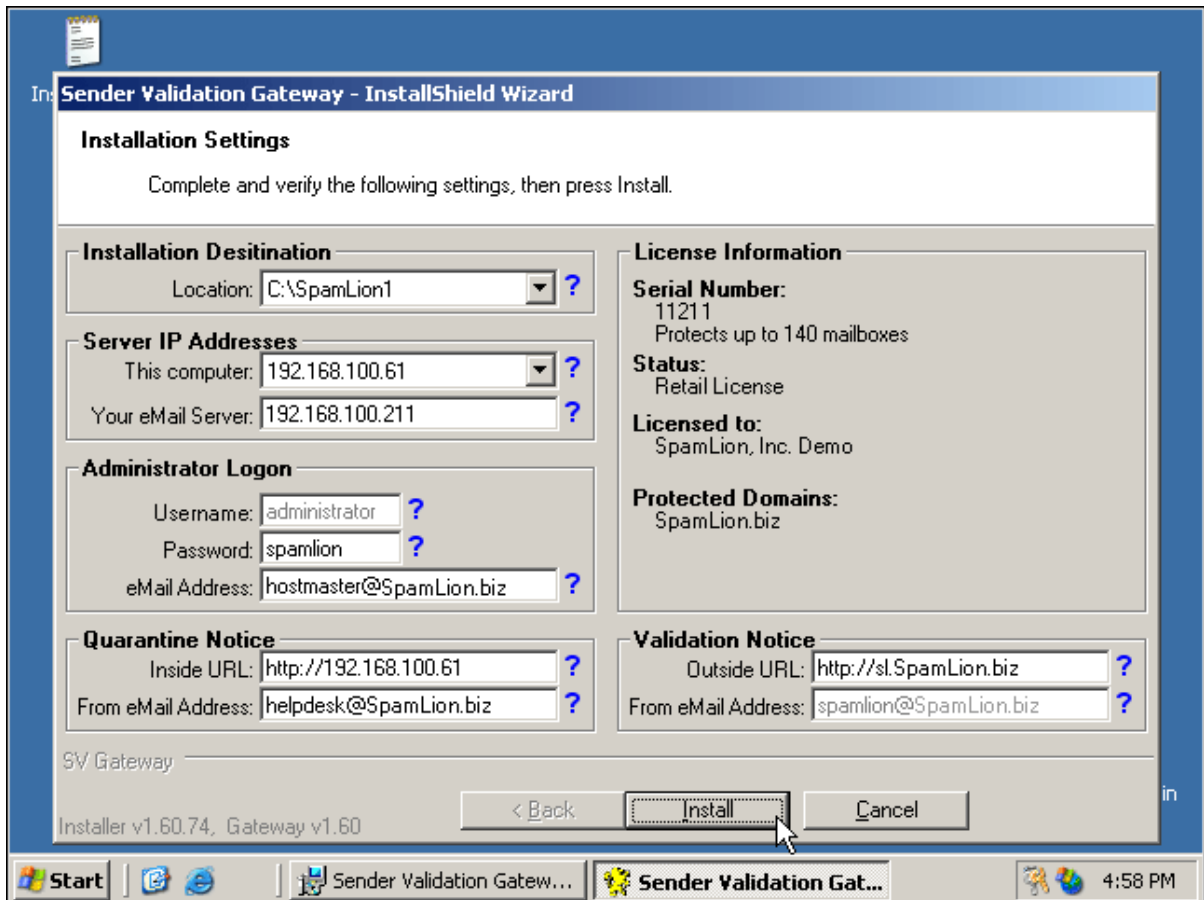


Figure 6, Gateway Installation Settings

2. Test and Cutover Outgoing Email

Using Telnet to create and send a message ensures direct connectivity between the Gateway, your email server, and the Internet, without disturbing live email flow.



Please see **KB-200509-1**, *Sending Test Messages Using Telnet* for details.

1. Test Outbound Path

You need to ensure that email sent from your email server to the Gateway will be delivered through your firewall to the Internet.

Using Telnet, send the first test message from the **command-line console of your email server** to an external email address, such as Yahoo or Hotmail account.



See **KB-200509-1** for more detail on using Telnet to create test messages.

Test Outbound Path (continued)

Please note:

- This will **only** work properly from the console of your email server.
- What you type is in **bold** (below).
- Use the Gateway's IP address instead of the example of 192.168.100.61
- The Gateway will respond with your email server's address instead of 192.168.100.211
- Use your real "from" email address
- Choose a real "to" email address such as a Hotmail or Yahoo account.

Example:

```
C:\> TELNET 192.168.100.61 25
220 sl.spamlion.biz Microsoft ESMTMP MAIL Service, Version:
5.0.2195.6713 read at Tue, 13 Sep 2005 11:12:01 -0700
helo mail.spamlion.biz
250 sl.spamlion.biz Hello [192.168.100.211]
mail from: test@spamlion.biz
250 2.1.0 test@spamlion.biz....Sender OK
rcpt to: receiver@domain.com
250 2.1.5 receiver@domain.com
data
354 Start mail input; end with <CRLF>.<CRLF>
subject: test one

This is my first outgoing email test.
.
250 2.6.0 <SL1jrEP6c0WMVFsOfsx0000001a@sl.spamlion.biz> Queued
mail for delivery
quit
221 2.0.0 sl.spamlion.biz Service closing transmission channel
C:\>
```

2. Check the IIS SMTP Log

Locate the logs at \SpamLion1\LogFiles\SMTPSVC1, and find two groups of entries:

- Reception of the message from your email server
- Transmission of the message to the Internet

If there is no 2nd entry (Transmission to the Internet), most likely your firewall is not allowing the Gateway to send outbound SMTP; also check DNS and restart IIS's SMTP service. A firewall, networking, or IIS SMTP expert may be needed to help resolve any transmission issues.

3. Cutover Outgoing Email

After you've verified that the message was received by the external email account, you can change the Smart Host entry on the Exchange Server to route outbound email to SpamLion.



KB200509-3 shows where to find Exchange's Smart Host setting.

Lastly, create a message from Outlook (or your regular email client) and send it to test the Smart host setting. (You may need to first restart Exchange's IMS service.)

3. Setup and Test Inbound HTTP

Set up access from the Internet to the Gateway's website by defining a rule on your firewall, as determined in the chapter on **Preparation**.

Verify the Gateway's website can be accessed from the Internet by connecting to the **Outside URL** from the Internet (not your local LAN – if you have to, call a friend or SpamLion, Inc.).

4. Test and Cutover Inbound Email

1. Test the *Internal* Inbound Path (Gateway to your Email Server)

Send a Telnet test message from the **console of the Gateway** to your email server (preferably your email address).

This is very similar to the Outbound test, only this time you:

- Use the Gateway's console
- Connect to your email server's IP address
- Say hello from the name of the Gateway (for example, sl.spamlion.biz)
- See the Gateway's IP address on the connection confirmation
- Interchange the "to" and "from" addresses

2. Check the IIS SMTP Log

Locate the logs at \SpamLion1\LogFiles\SMTPSVC1, and find one group of entries:

- Transmission of the message to the your email server

3. Cutover Inbound Email

Once you have verified the message was received, change the firewall rule to route inbound Internet email to the Gateway.

4. Test the *External* Inbound Path (Internet to Gateway)

To verify the Firewall is truly sending inbound email to the Gateway, send a test from an external email account (Hotmail, Yahoo, etc.) to the Receiver you've been using for testing (your address).

5. Finally, check the IIS SMTP Log

Locate the logs at \SpamLion1\LogFiles\SMTPSVC1, and find both groups of entries:

- Reception of the message from the Internet:
- Transmission of the message to your email server.



For more detail on reading logs refer to **KB200308-3**, *Message Tracking*.

Additional Installation Features

1. Synchronize Receivers' Email Addresses – Microsoft Exchange

GALSync - Global Address List Synchronization

This process can manually or automatically synchronize all **Primary and Alias** addresses. These utility and batch files are used to run Microsoft's **GAL Export** utility, which is included with Microsoft Exchange. Then the output file is placed in \SpamLion1\xfer\sync.

Key Features

- 1) Combines each **Primary email address** with its **Alias(es)** to provide a single managed Quarantine for each user.
- 2) Enables protection against **Dictionary Attacks**.

The GALSync can be manually performed, or run at an interval of your choosing using the Windows Scheduler.



Before running the first GALSync, determine if the majority of the users will be Protected. If so, change the default for **New Receivers'**, which is found in the Administrator console – Settings – Processing – **New Receivers' Default Settings, Protection**. Remember to set the default back to "Bypassed" when done.

Running Manual GALSync with Exchange server:

1. Copy the appropriate folder from SpamLion1\GALSync (Exchange 5.5 - GALSyncEX55, Exchange 2000 - GALSyncEX2K, or Exchange 2003 - GALSyncEX2003) to the appropriate Exchsrvr folder on the Exchange Server (usually C:\exchsrvr, but it might be in c:\Program Files\Exchsrvr, or on a different drive).
2. Open a command line window and navigate to the folder you just copied.
3. Run the initial export, by typing "ADE /extract user /m" from a command line.
4. Copy the output file, "**slconverted.txt**" to the folder "\SpamLion1\XFER\Sync" on the Gateway. Though unnecessary, feel free to inspect and edit the file "SpamLion Address List Synchronization.pdf".
5. Once placed in the \SpamLion1\XFER\Sync folder, the Gateway will see the file and automatically import it within a few seconds. Log on to the Gateway as *Administrator* and check that the Receivers were created - you probably need to click on the "**Include Bypassed**", and press **Search**, to see them.

For Automated GALSync with Exchange server:

1. Create a local security account for the GALSync, example: GALSync.
2. Set the NTFS permission to Modify, on the SpamLion1\Xfer\Sync folder to include the GALSync security account.
3. Create a share called "Sync\$" on the SpamLion1\Xfer\Sync folder and set share permissions to **Full Control**.

For Automated GALSync with Exchange server (continued)

6. Copy the appropriate folder from SpamLion1 \GALSync (Exchange 5.5 - GALSyncEX55, Exchange 2000 - GALSyncEX2K, or Exchange 2003 - GALSyncEX2003) to the appropriate Exchsrvr folder on the Exchange Server (usually C:\exchsrvr, but it might be in c:\Program Files\Exchsrvr, or on a different drive).
7. Modify the ADE.BAT file to the correct share, userid and password that you have created previously.
4. Initial Receivers update using the ADE.Bat file.
5. Run the initial export. Type: "ade /extract user"
6. Log on to the Gateway as Administrator and check that the Receivers were created (You may need to click on the "Include Bypassed", and press **Search**, to see them).



If there are any problems, check that the Scheduled Task has permissions appropriate to run an LDAP query, create files, connect to the network share, and transfer the file.

7. Use the Windows Scheduler to have this batch file run daily, or run it whenever you've made changes to the email accounts on your Exchange network.

Export Active Directory Contacts as Receivers (Optional)

Some organizations define email-enabled identities in their Active Directory. These identities do not have a mailbox on the Exchange Server; however, they have a email identity on the email domain. The purpose of these identities is to forward email to another address. Inbound email sent to this type of identity is immediately forwarded to another email address. If you want to protect this type of entity you may either enter the address manually in the Receivers page or use the ADE utility to transfer them from AD to SpamLion. The following steps rely on the share, permissions and user login id created in the previous step:

1. Modify the ADE.BAT file to use the correct share (Sync\$), userid (GALSync) and password that you have created previously.
2. Type "ade /export user contactasreceiver"

Just as with Automated GALSync, you can schedule this task to occur regularly.

2. Synchronize Receivers' Email Addresses – Other Email Servers

Automatic Discovery

The Gateway will automatically discover the *primary* email address of each person by monitoring outbound email.

Alias addresses are discovered by monitoring incoming email, providing them with a separate quarantine. To combine them, perform an Automated or Manual GALSync.

Manual GALSync

Either have your email server export a list of *primary* and *alias* email addresses, or create a text file (shown in the example below). Then place this file in the \SpamLion1\Xfer\Sync folder.

The format is, one entry per line:

[primary email address] [Tab key] [alias1] [Tab key] [alies2] [Tab key] [alies3] ...repeat

Manual GALSync (continued)

For example:

```
dlyon@spamlion.biz
john.doe@spamlion.biz    accounting@spamlion.biz
mary.doe@spamlion.biz
sam.smith@spamlion.biz
jane.doe@spamlion.biz    sales@spamlion.biz
rbest@spamlion.biz
```



For more information on GALSync with *non-Exchange* servers, see **KB200509-6**.

3. Enable Dictionary Attack defense

After all Receivers (and aliases) have been discovered, created, or synchronized, log on to the Administrator console – Settings – Notices – Non-Deliverable Inbound Mail section, and enable (check) the “**Reject mail to non-existent Receivers**” feature.

Leave “**Send NDRs to Invalid Senders**” unchecked to discourage NDR Relay attacks and help prevent outbound NDR congestion. Note: Regardless of this setting, the Gateway will NOT return the original message in its NDR Notice, so such attacks will be fruitless for spammers.



Valid Senders will receive NDRs if they misaddress mail to your staff (Valid Senders are not effected by the Send NDR feature).

4. Customize the Welcome Notice (Validation/Registration Notice)

First open a browser using the Inside URL, and **logon as the Administrator**. (Check the box “SpamLion Administrator” and click “Submit” to have the password field appear).

Default Username: **administrator**

Default Password: **spamlion**

Once logged on, select **Settings**. then click on **Notices**.

Feel free to modify the **Registration message**, we recommend:

- Click on **Help** for the most current information. (Help pages are from www.SpamLion.com, and will contain suggestions and samples used by other companies)
- Place your company’s phone number in the message
- Provide the <ONE_CLICK_URL> near the top, and on its own line (so that it stands out)
- The shorter the better

5. Automated and Manual Whitelisting

Automated Whitelist Discovery

By default, the Gateway will auto-whitelist all email addresses sent to by a **Protected** person. (This can be disabled on a per-user basis.)

Also, the Gateway *can* be set to auto-whitelist all email addresses sent to by a **Bypassed** person. To set this up go to Settings - Processing, and un-check the "Skip Outbound AutoValidate for Bypassed Receivers" feature. **This feature enables building a whitelist before turning on protection.**

Whitelist Sent Email Folders from Exchange

The learning process can be jump-started by extracting the addresses of everyone your staff has sent email to from their "Sent" folder in Exchange. This is ideal for companies who want an "instant whitelist."

The *Outlook Export and Upload Utility** enables your staff to instantly create and upload a whitelist of whom they have been communicating with. This secure and distributable utility enables the gateway to be deployed with a near perfect whitelist from the start. *Requires Outlook 2003.



Use the included *Outlook Export and Upload Utility* included with the product (in the Utility folder). Watch the video on <http://SpamLion.com/Demo>.



Refer to **KB200509-5** for instructions on how this is manually performed.

Manual Whitelist a Single Email Address

Using the Quarantine Manager or Administration website, click on Senders, type in the full email address, and press "Valid."

Manual Whitelist an Entire Domain

To whitelist a Domain, Log in as the Administrator (it can not be done from the Quarantine Manager) and type just the Domain Name (no special characters), for example **SpamLion.com**; however, be aware that approving a commercial domain, such as HotMail.com or Yahoo.com will dramatically reduce anti-spam effectiveness.

Whitelist Import Email Addresses

Simply create a list of addresses and use the Upload utility. Just skip step 1, because you're providing a list of e-mail addresses rather than extracting them from Outlook.

An Example of a list:

john.doe@spamlion.com
dan.lyon@stopuce.org
hostmaster@webhabitat.com



Use the included *Outlook Export and Upload Utility* included with the product (in the Utility folder). Just skip the first

Lists can also be directly imported on the server, without using the Upload utility by following KB200301-3 and formatting them as depicted below.



See **KB200301-3** for tips on how to easily create and format this file using Excel.

An Example of a direct import file:

```
x-sender: jane.doe@spamlion.biz
x-receiver: john.doe@spamlion.com
x-receiver: dan.lyon@stopuce.org
x-receiver: hostmaster@webhabitat.com
```



Please note, that for the Senders to be created as **Valid**, the first entry (**x-sender**) must be a **Protected Receiver's** email address. (Outbound messages have the sender/receiver labels reversed.)

Export Active Directory Distribution Lists

Some organizations have the list of external contacts organized as distribution lists within their Microsoft Active Directory. You can use the ADE utility to export the addresses and place them as valid senders in the SpamLion database.

Follow the steps listed below:

1. Using the SpamLion Administrator console Receivers page, insure that you have a protected Receiver with Validation set to "Company." It may be the Administrator account, for example: administrator@mycompany.com.
2. Set the NTFS permission to Modify, on the SpamLion1\Xfer\Xfer folder to include the GALSync security account.
3. Create a share called "Xfer\$" on the SpamLion1\Xfer\Xfer folder and set share permissions to **Full Control**.
4. Modify the ADE.BAT file to use the correct share (Xfer\$), userid (GALSync) and password that you have created previously.
5. Type "ade /export contact administrator@mycompany.com"

Note: This is very similar to GALSync; however, it exports to the \SpamLion1\Xfer\Xfer folder (not the Sync folder), and it formats its output as specified for Whitelist Import (above).

Import Outlook and/or Outlook Express Contacts as Valid Senders

In the event that your contacts are not in Active Directory, you may want to import Outlook and/or Outlook Express contacts from each user's own address book to SpamLion.



Refer for detailed instruction in the **KB200302-1, Contact Import**.

Please note that for the Senders to be created as **valid**, the first entry (**x-sender**) must be a **Protected Receiver's** email address. (Outbound messages have the sender/receiver labels reversed.)

6. Configure SMTP Email Delivery Settings

For Performance

In companies with high traffic volumes, the outbound email re-try queue may grow to a size that impacts IIS's performance. In order to reduce the possibility of this happening, make the following adjustment to the settings found in IIS Manager, SMTP Virtual Server **Delivery** property. Change the settings to correspond to the ones in Figure 6.

For Failover

Alternately, changing the **Expiration timeout** to 3 days, will hold all messages in queue for up to three days, should Internet access be lost or your email server becomes inoperable. The trade-off is that Welcome Notices to non-existing Senders will be queued for up to three days – in high-traffic situations this can cause a minor performance impact.

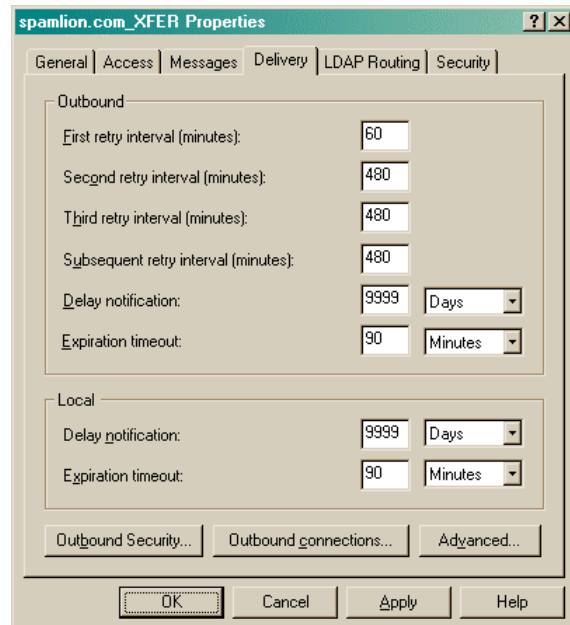


Figure 6, IIS's Performance SMTP Settings

7. Defining Additional Domains

Adding Protected Domains

If you wish to also Protect mailboxes in this new domain, submit a support ticket to SpamLion, Inc. to have your license file reissued to include the new domain. A Standard support fee is normally required, and the Domain must be fully owned and operated by your company (other restrictions may apply).

After obtaining the new license file, follow the instructions under *Replacing the License File* in the *Licensing* chapter of this document, and then continue on to configure IIS.

If you **do not** want to protect the additional domain, no change in the license file is required, as the Gateway automatically passes all email through that are for unprotected Domains.

Configuring IIS SMTP

Using IIS's MMC (Microsoft Management Console), add a Remote Domain, set it to allow Incoming email, and then enter your Email Server's IP address, in square brackets, in the **Route Domain** to "Forward all email to smart host" setting.



See **KB200509-7**, *Defining Additional Domains*, for a step-by-step procedure of how to configure IIS's SMTP service to accept incoming mail for other domains.

Deployment

Partial Versus Company-wide Protection

The Gateway can be set to protect no one, a select few, or everyone in your company, simply by selecting which email addresses to protect (versus bypass).

Understanding “First Contact” Protection

The Gateway **only Quarantines** email from, and sends a *Notice* to a **First Contact** – no one else.

The Gateway’s unprecedented accuracy comes from using the **firewall paradigm**: “allow all known responses back in, question only the unknown” - all *first contact* email is unknown.

Several email communication studies have show that over 99.99% of *First Contact* email is spam, but more importantly, that *non-First Contact* email was **not spam**.



Automatically learn with whom your company communicates and allow that mail through. Over 99.99% of **everything else is spam**.

Validating the One in Ten Thousand *Real* First Contacts

Simply let people know that email from someone new will need to be one-time validated, and that there are several easy ways to do this:

- The Sender clicks on the One-Click Validation link in the Welcome Notice
- The Sender replies to the Welcome Notice
- You manually Validate them by using the Quarantine manager
- Someone (or something) at your business sends them an email



Feel free to customize our user guide template to your preference. It’s written in Microsoft Word and located in the SpamLion1 \ Documentation folder.

Additionally, check our website for Instructional Videos.

Eliminate First Contact Validations for Existing Customers and Vendors

Please refer to *Additional Installation Features – 5. Automated and Manual Whitelisting*.



Update your company’s website – instead of displaying email addresses, use an information gathering form, then relay the form’s confirmation through the Gateway.

- This will auto-whitelist new customers
- More importantly, it’s not about auto-whitelisting; it’s about better understanding your customer’s needs when they first contact you.
- Read **KB200509-4** for more information.

Staged Rollout

Regardless of how you build your initial whitelist (learning or importing), most companies find it easier to deploy a new product to groups of users, rather than the entire company all at once.

To facilitate a staged rollout without burdening the administrator or IT department, just ask groups of people to connect to the Gateway's website and enter their email address, connect to their Quarantine Manager with the One-Click Logon, and select "Protected." Just as with any company-wide rollout, only without the administrative overhead.

Restricting Use

You may also restrict users from changing their settings (such as enabling or disabling protection) by altering the **Receivers' User Interface Settings** via the Administrator console's Settings, Processing page.

Consulting Services

To ensure a trouble-free installation, please leverage the expertise of an authorized Reseller or Partner.



The guidance an experienced SpamLion Reseller / Partner can provide can be of great value. Whenever installing a system that can potentially affect everyone within your organization, seeking the assistance of someone who has previously performed such work is highly recommended.

Maintenance

Automated Housekeeping

The following maintenance tasks are performed at time intervals you set:

- Purges unclaimed Quarantine and Trash
- Removes Invalid Senders who no longer send you email
- Purges unused One-Click Validations and One-Click Logons
- Automatically backs up and packs the Microsoft Jet database
- Automatically purges old log files and backup databases

Log Files

After the first week or so, please turn off IIS's Logging, and set SpamLion's logging to minimal.

Backups

The most critical data to backup regularly is:

- Gateway's database: /SpamLion1/Database/spamlion.mdb
(Feel free to delete the auto-backup files (SpamLion.###.mdb))



Please follow **KB200301-6** to snap-shot the database (do not attempt to backup the live database while the Gateway is running).

You should also make a copy of:

- customized logon or registration pages:
 - /SpamLion1/Web/login.htm
 - /SpamLion1/Web/register.asp
- installation software
- license file

There is no need to backup the Quarantine folder, being it's all from unknown sources.

Software Updates

SpamLion, Inc. regularly improves the Gateway's performance, user interface, and adds capabilities beyond blocking normal spam. For example, future releases are planned to stop Identity Theft Relay, invalid NDR's, and Phishing.



An annual subscription to Software Maintenance is required to obtain updates and 50% off technical support.

Licensing

Trial License

The system is **fully functional** during any trial period.

After the first two weeks, the Gateway will notify the administrator once each day about the number of days remaining with the current license. When you've accepted the product (or completed the 30-day satisfaction guarantee period), simply notify your Gateway vendor finish the purchase and obtain a non-expiring license.

If the License Expires

The Gateway will switch into "full bypass" mode, and pass all email through the system without any protection. **Email flow will not be interrupted**, but be prepared for complaints from your staff, as no other anti-spam product can provide such unprecedented protection.

Replacing the License File

Simply replace the existing license: `\SpamLion1\Engine\SpamLion.lic`, with the permanent license. Then stop and restart the SpamLion service. Make sure that you save this new license in a secure place as part of your backup procedure.

Copy Protection

The product is constrained to protect a **limited number of mailboxes** (alias addresses are not counted), for **only the Internet Domains owned by your company and used by your staff**.

To increase the number of protected mailboxes (users), or to add another registered domain, contact your Reseller/Partner to purchase the additional license(s). When your purchase is complete, they will send you a new License File, which you'll replace as previously described.

Uninstall



If you plan to ever reinstall the Gateway, please make a Backup as described in the Maintenance Section of this guide.



Before removing the Gateway, restore mail routing to its original configuration.

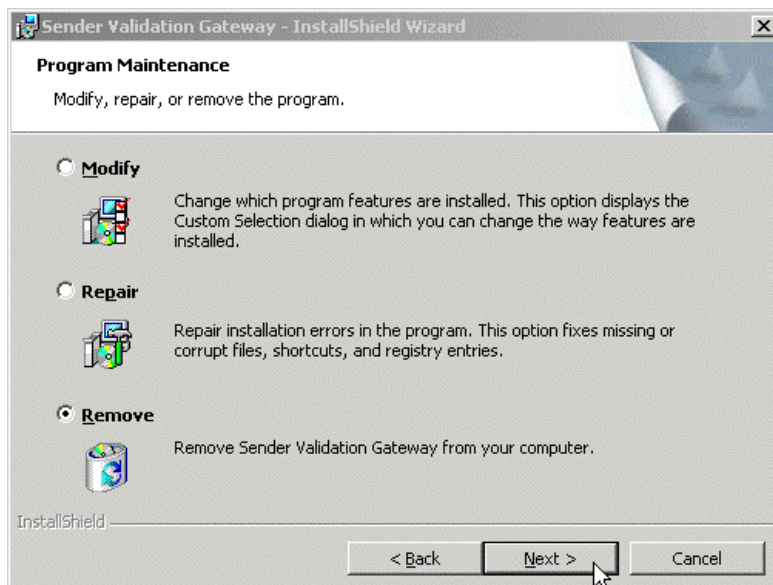
- Set your firewall to route inbound mail to your mail server.
- Change the Smart Host entry on your mail server to no longer send outbound mail through the Gateway.
- Test the changes to ensure mail is **flowing directly** to and from your mail server (no longer through the Gateway).



In some instances, InstallShield® may not operate properly when using *Add/Remove Programs*, therefore running **Setup.exe** and **selecting the Remove** option is a best practice. If you have difficulties, follow the Manual Removal process covered later in this section.

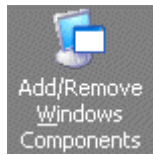
Typical Removal

1. Ensure email no longer flows through the Gateway by reconfiguring your firewall and email server.
2. Launch Setup.exe, just as done when installing the program.

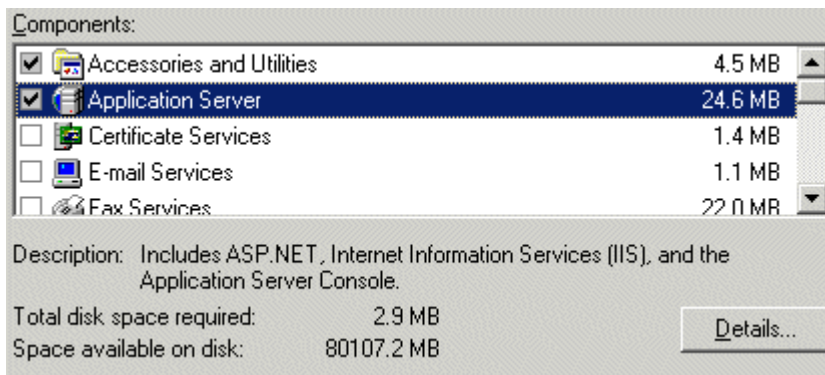


3. Select the **Remove** option, press **Next**, and wait for the remove to complete.
4. If you have other websites (or FTP sites) on this server, and are planning to re-install the Gateway, then record their setup information, as you will need to redefine them after you reinstall IIS and the Gateway.

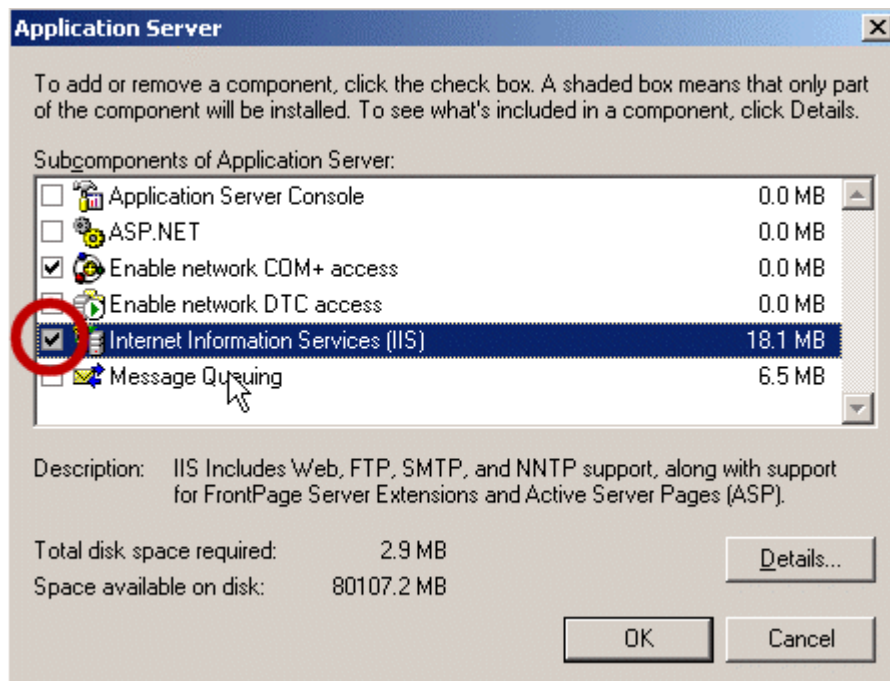
If you are not planning to reinstall the Gateway, then there is no need to remove IIS (do **not** continue on to step 5, unless planning to reinstall the Gateway).



5. Launch **Add/Remove Programs** from the **Control Panel**.



6. Select **Application Server**, and press **Details**.



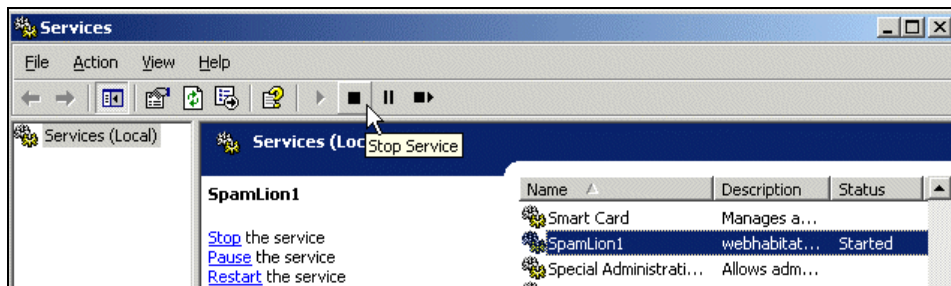
7. Un-click **Internet Information Services (IIS)**, and select **Ok**, and then **OK** again on the next window, and close the IIS MMC when finished.

- When re-installing the Gateway, follow Appendix I or II to properly reinstall IIS first.

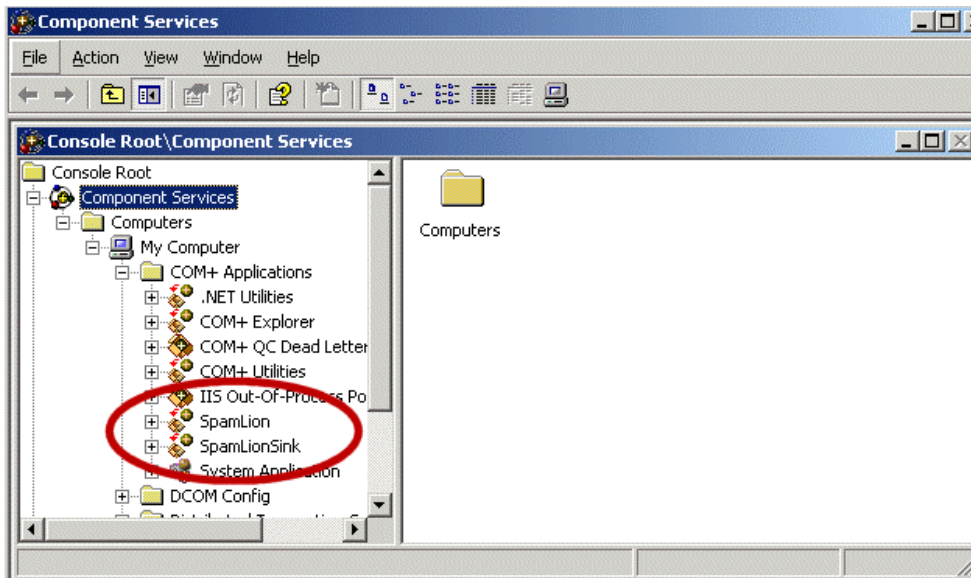
Note: The Gateway will not re-install properly if IIS is not completely uninstalled and re-installed, because uninstalling the Gateway removes its Virtual Servers from IIS, and you must reinstall IIS to have them recreated.

Manual Removal

Should the Typical Removal Fail, or if you just want to ensure the Gateway is completely removed from the system, check that each of the following steps has been completed.

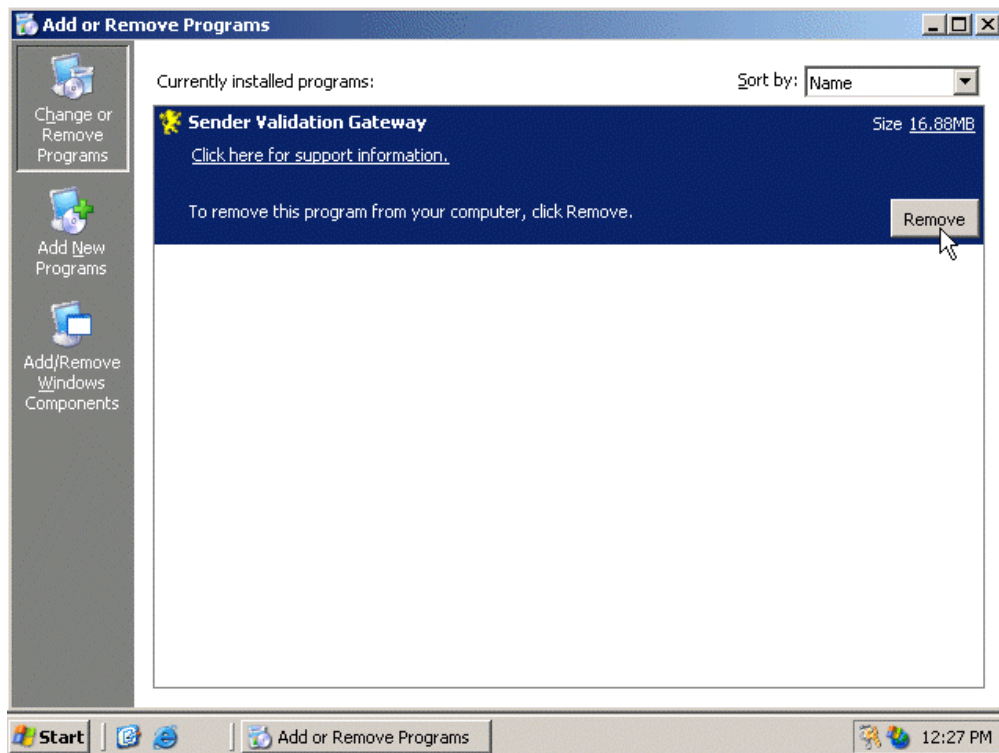


1. Stop the **SpamLion1** Service (if it was not removed).



2. Open **Component Services** MMC (Administrative Tools, Component Services), and navigate down to: **Computers\My Computer\COM+ Applications**
3. Ensure the **SpamLion** and **SpamLionSink** COM+ Applications were deleted by **right-clicking** on them and selecting **Delete**. Then close the Component Service MMC Window.
4. Launch REGEDIT.EXE and ensure the following entries are no longer in the Registry:
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\SpamLion1
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SpamLion1

(Improperly editing the Registry can result in complete failure of the system, ensure you are only deleting only these two keys.)



5. Select **Add/Remove Programs** from the **Control Panel**, and **Remove** the **Gateway** if it is listed. Then complete steps 3 through 7 in the above section **Typical Removal** to remove the InstallShield's Setup and IIS's custom configuration.

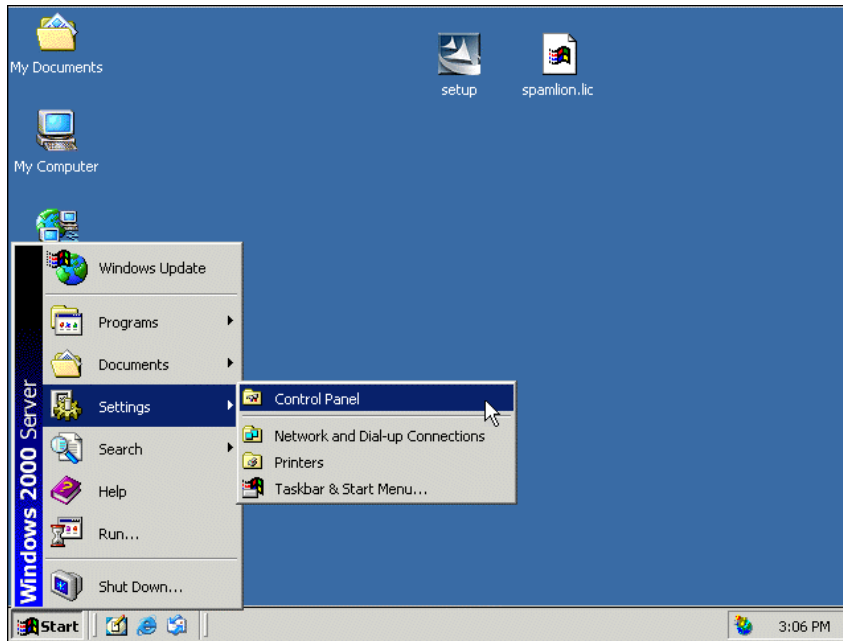
6. Ensure both folders have been removed:
 - a. \SpamLion Product (Installation files)
 - b. \SpamLion (the Gateway program and Quarantine)

7. Reboot the system

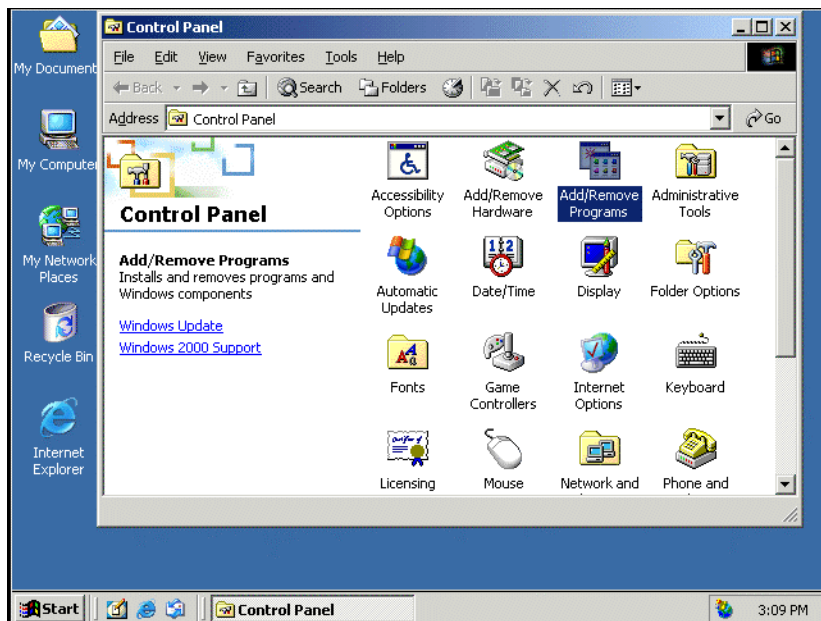
Appendix I (IIS 5.0)

IIS 5.0 Setup for Windows 2000 Server, Advanced Server, Windows Professional, or Windows XP

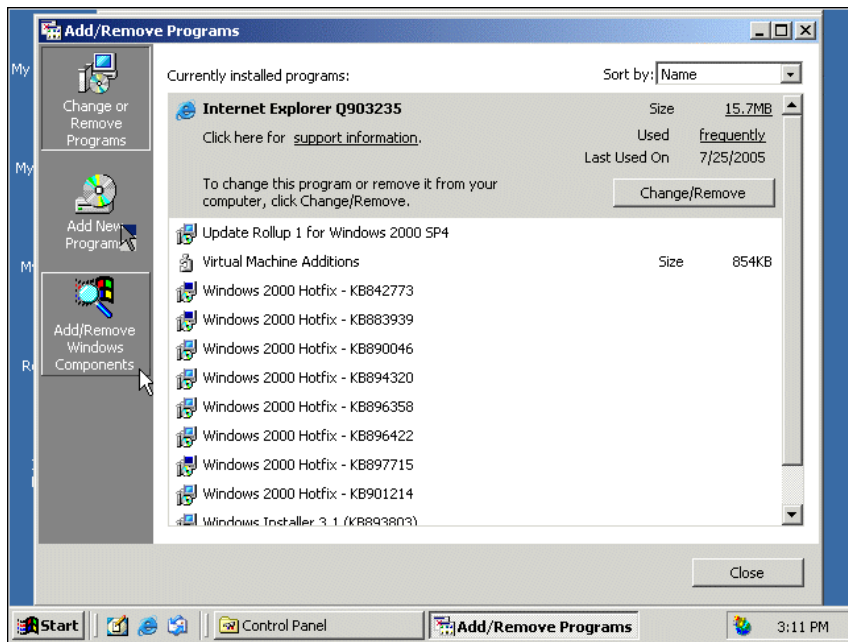
Please follow the following steps precisely to simplify installation of the Gateway. **If IIS has already been installed, it's best to remove it and re-install it exactly as shown below.**



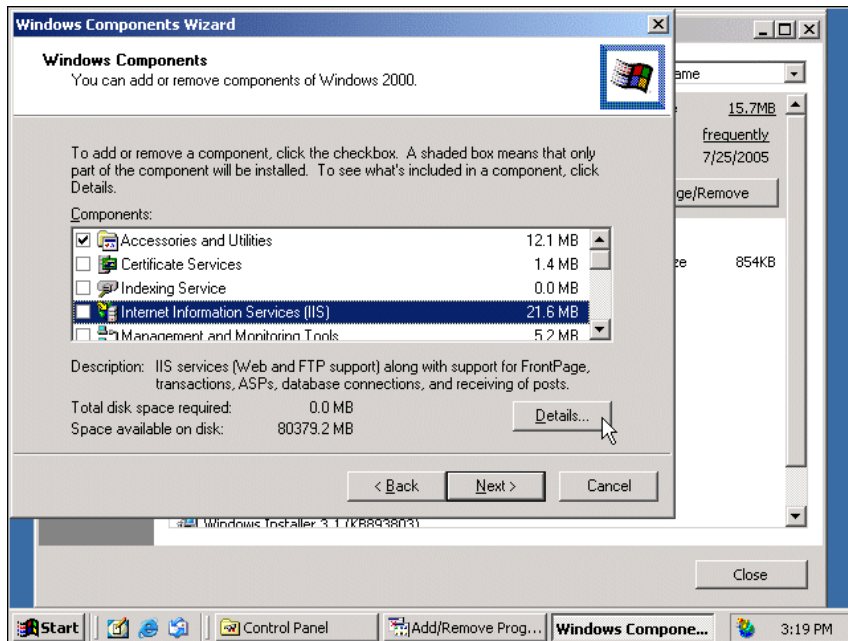
1. From the **Start** button, select **Settings**, and then **Control Panel**.



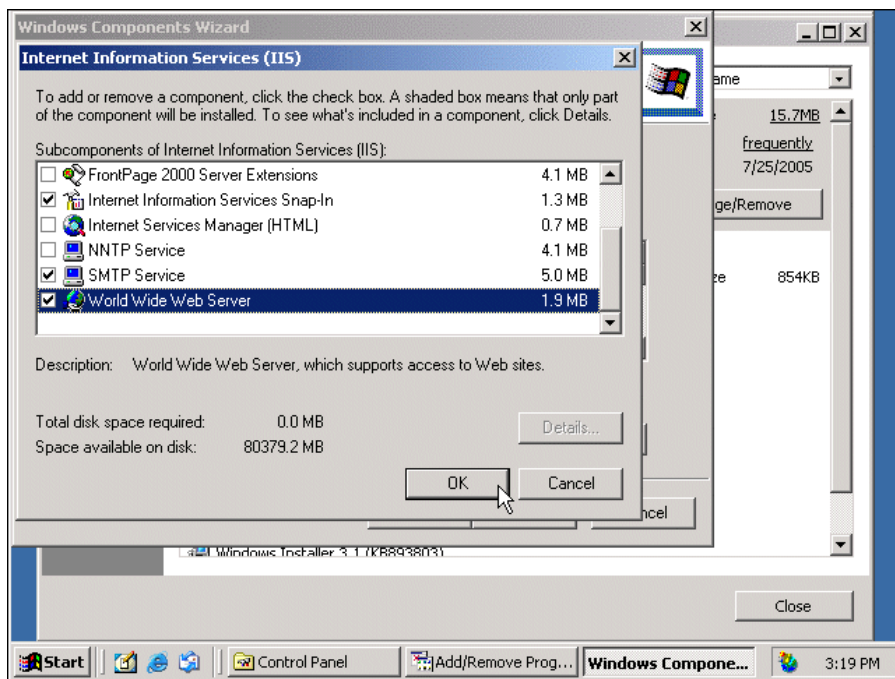
2. Click on **Add/Remove Programs**.



3. Click on **Add/Remove Windows Components**



4. *Select* (NOT check) **Internet Information Services (IIS)**, and click on **Details**

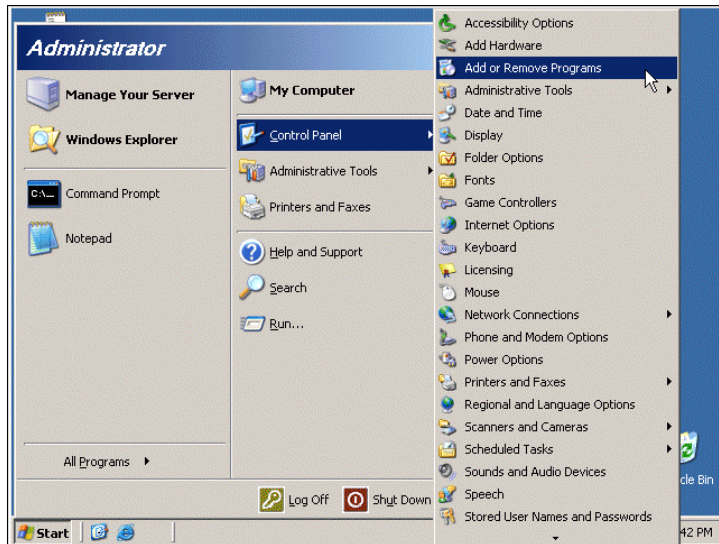


5. Check **SMTP Service**, and **World Wide Web Server**, then click on **OK**.

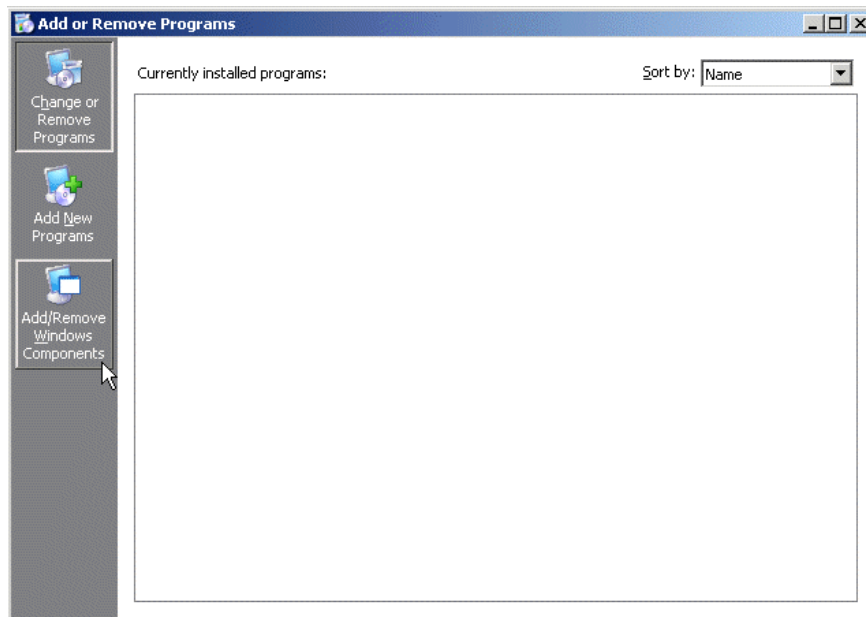
6. Continue to click on **OK**, to close all the previously opened windows, then close the *Add/Remove Programs* window.

IIS 6.0 Setup for Windows 2003 Server – Standard or Enterprise

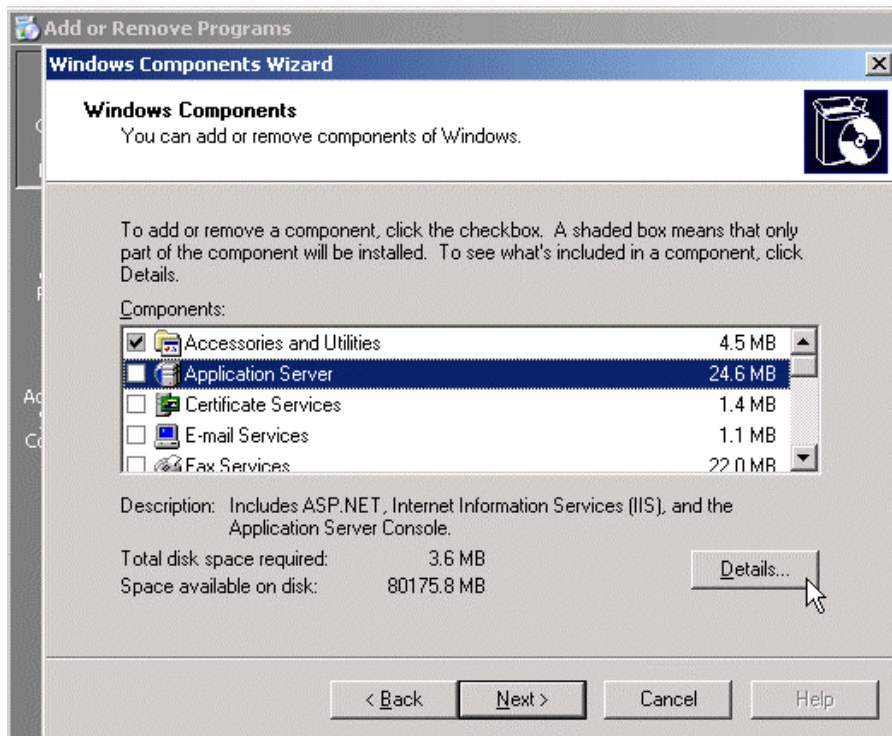
Please follow the following steps precisely to simplify installation of the Gateway. **If IIS has already been installed, it's best to remove it and re-install it exactly as shown below.**



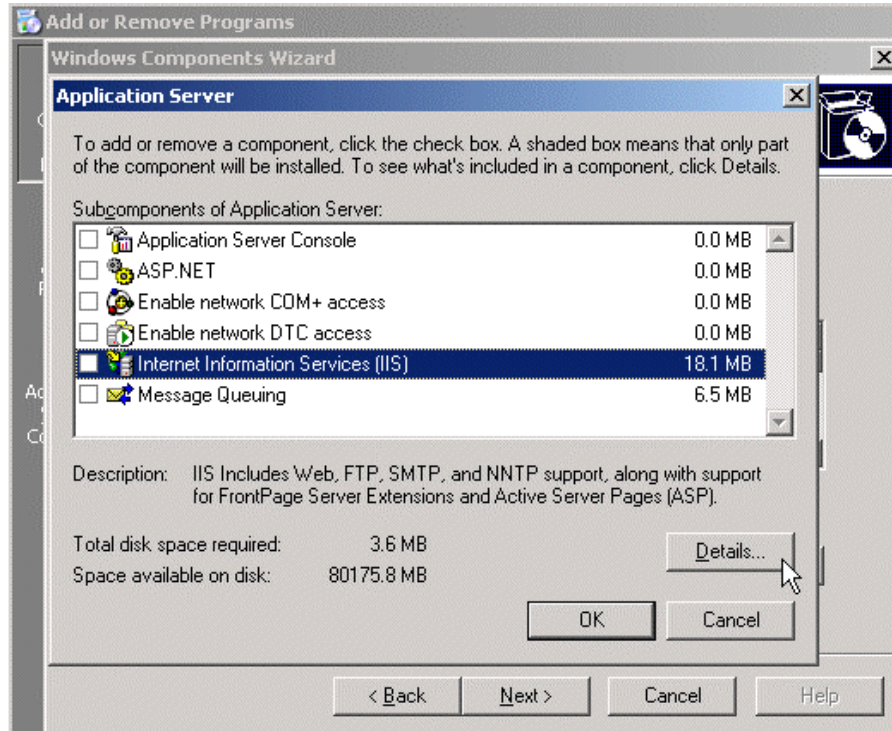
1. From the **Start** button, select **Control Panel** and then **Add / Remove Programs**.



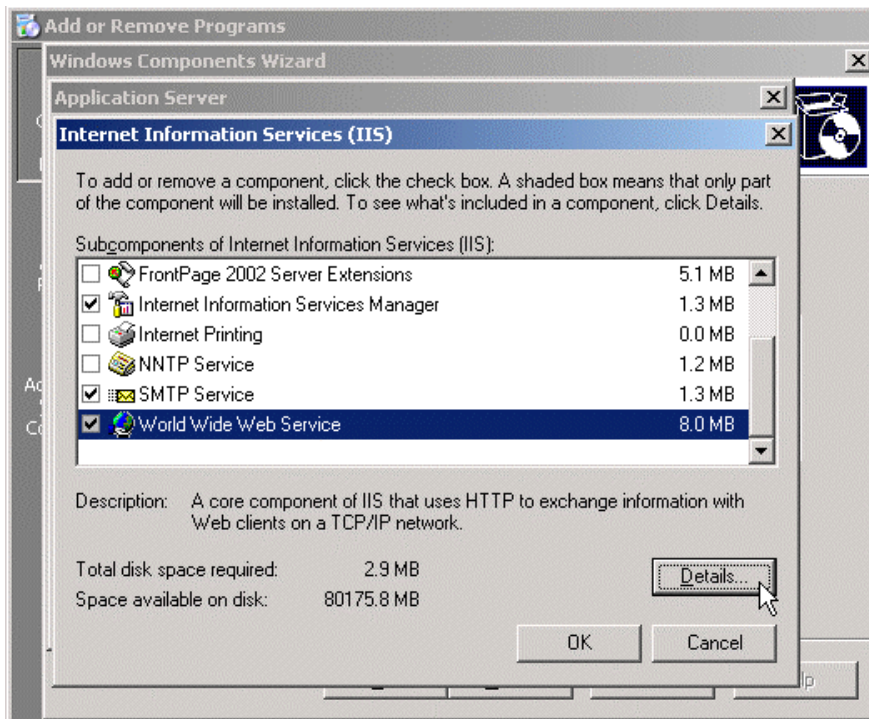
2. Click on **Add/Remove Windows Components**



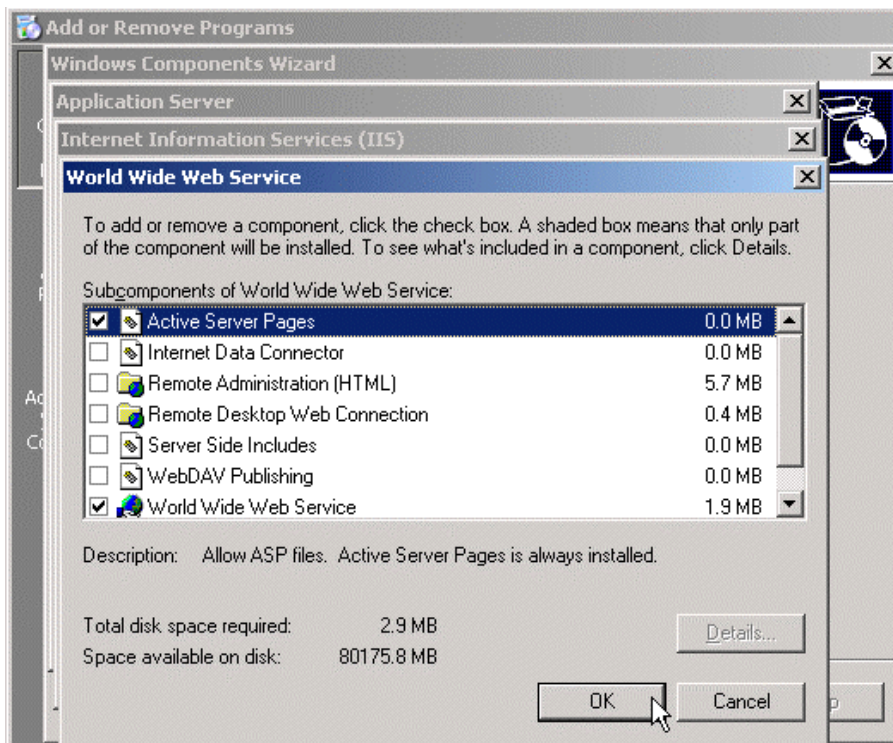
3. Select (NOT check) **Application Server**, and click on **Details**.



4. Select (NOT check) **Internet Information Services (IIS)**, and click on **Details**.



5. Check **SMTP Service**, and **World Wide Web Service**, then click on **Details**.



6. Check **Active Server Pages**, and click on **OK**.

7. Continue to click on **OK**, to close all the previously opened windows, then close the *Add/Remove Programs* window.