

AbleServer.com



Mail Services Users Guide

Version 2.1.1

Table Of Contents

| | |
|--|-----------|
| <i>Introduction</i> | 4 |
| Quick Start Instructions | 4 |
| <i>Web Based Administration</i> | 5 |
| Postmaster Address | 5 |
| Email Accounts | 5 |
| Aliases Forwards | 6 |
| Autoresponders | 6 |
| <i>Domain Name Changes</i> | 7 |
| MX Record Change | 7 |
| Host Name Branding | 7 |
| <i>Email Client Configuration</i> | 8 |
| POP3 Settings | 8 |
| <i>Webmail</i> | 9 |
| Accessing Webmail | 9 |
| Supported Languages | 9 |
| Webmail Features | 9 |
| <i>Anti-Virus Scanning</i> | 11 |
| Introduction | 11 |
| How It Works | 11 |
| Anti-Virus Scanner | 11 |
| <i>SPAM Filtering</i> | 12 |
| Introduction | 12 |
| Filter Common SPAM Activity | 12 |
| Email Content Filtering | 12 |
| SpamAssassin | 13 |
| <i>Getting Support</i> | 14 |
| <i>Appendix</i> | 16 |
| Hardware and Software Used | 16 |
| Preventing SPAM | 18 |
| How To Stop Address Harvesting on Your Web Site | 19 |

Introduction

Quick Start Instructions

We recommend a careful review of this User Manual, because it will help you to get the most out of your new Mail Services. There are several features that require the more detailed explanations found in this manual.

However, if you wish to get started immediately, you can do the following:

1. Create the mailboxes: The Domain Administrator can be found at this location:

<http://mail.ablehost.com/domainadmin>

Using the username and password provided to you, you can begin adding new mailboxes through the Domain Administrator.

2. Modify Domain Name MX Record: Ask your ISP or web hosting company to change your domain's MX record to:

mx.ablehost.com

After this has been changed, all email going to your domain name will be routed to the mailboxes you created on our mail server.

3. Configure POP3 Email Software: Configure your POP3 email software so that it will download your email from our server. Use these settings when configuring popular desktop email clients.

Incoming (POP3) Server: **mail.ablehost.com**

Outgoing (SMTP) Server: **relay.ablehost.com**

Username: **user@domain.com** (user's FULL email address!)

IMPORTANT: Set the option "Outgoing Mail Server Requires Authentication". This is usually presented as a check box in Email client configuration and is necessary for outgoing mail to function.

Web Based Administration

When your account has been established you will be given a designated number of mailboxes that you can establish within your account. Using the web based administration, you will be able to add mailboxes, add aliases and other functions.

To access the Web Based Administration, open up a web browser and go to:

<http://mail.ablehost.com/domainadmin>

You can also access it via SSL (recommended):

<https://mail.ablehost.com/domainadmin>

Enter your domain name, and the postmaster password assigned to you.

Postmaster

We have already created one mailbox for you, which is postmaster@yourdomain.com. This is the mailbox used for logging on to the web based administration. Internet standards recommend that every domain has a functioning postmaster address. We recommend you keep this email address or forward it to another address. You have not been charged for this mailbox.

Email Accounts

To view the email users for a domain click on "Email Accounts", from the main menu of the Domain Administrator. This lists all of the email users for the domain. You can scroll through them using the index at the bottom of the page. The number of current users vs. allowed users is displayed at the top of the page.

One email account for each domain can be defined as a catchall account. This account will receive all of the email that was addressed to the domain that could not be delivered. You can also select to have undeliverable email deleted, bounced (returned to sender), or forwarded to another address using the links at the bottom of the "Email Accounts" screen. The default setting is to bounce undeliverable messages.

To modify an existing user, click the "Modify User" button. From this screen you can change the user's password, forward their email, and turn on a vacation message.

To add a new email account click "Create Email Account" at the bottom of the "Email Accounts" screen.

Aliases Forwards

To view the aliases and forwards for your domain click on "Aliases Forwards" from the main menu of the Domain Administrator. A user with an alias can receive email addressed to them or the alias. Forwards allow you to forward email addressed to a specified address at your domain to any Internet email address.

Autoresponders

To add and edit autoresponders click on "Autoresponders" from the main menu of the Domain Administrator. Autoresponders send an automatic reply when email is received at a specified address.

Domain Name Changes

To bring your new email accounts online, there is one remaining task. You must make an entry into your domain name record. This is usually done by whoever is listed as the Technical Contact on your domain name (usually your ISP or your web hosting company).

MX Record Change

There is a special record for each domain called a MX Record, and it defines the host responsible for that domain's email. If you manage your own DNS, you can simply change the MX Record using the directions below. Otherwise, you will need to contact your ISP or web host and ask them to make the change. It is a very easy change to make.

You will need to ask that the entry below be placed in your MX record. Once this is done, any email addressed to your domain name will be routed over to your new mailboxes.

mx.ablehost.com

If for some reason, you do not wish to take advantage of the anti-virus scanning and the SPAM filtering, then you should enter this into your MX record instead of the one above:

mx-noscan.ablehost.com (no virus or SPAM filtering)

Host Name Branding

If you wish to have your own name used for the mail server (instead of mail.ablehost.com), ask your DNS administrator (usually your ISP or your web hosting company) to add the four CNAME records below to your domain. CNAME records act as aliases and allow you to use your own host names in place of the ones assigned by us.

Here is a recommended strategy:

mail.yourdomain.com CNAME **mail.at.ms.ablehost.com**
relay.yourdomain.com CNAME **relay.at.ms.ablehost.com**
mx.yourdomain.com CNAME **mx.at.ms.ablehost.com**
mx-noscan.yourdomain.com CNAME **mx-noscan.at.ms.ablehost.com**

Email Client Configuration

Any popular POP3 email client (software on your computer for accessing your email) can be used to access your email. We recommend Microsoft's Outlook Express for use on Windows desktops. The information below will explain how to set up and configure your email program for POP3 access to your email.

POP3 Settings

These are the settings to use in your email software:

Incoming (POP3) Server: **mail.ablehost.com**
Outgoing (SMTP) Server: **relay.ablehost.com**
Username: **user@domain.com** (use FULL email address!)

Outgoing Mail Server Requires Authentication: (IMPORTANT) You must indicate in your email program that your Outgoing Mail Server Requires Authentication. This is usually presented as a check box in email client configuration and it is a required setting. If you are prompted for a username and password for SMTP authentication in your email program, use the same username (full email address) and password that you use for POP authorization.

Using POP over SSL: Your Mail Services support POP over SSL, and we highly recommend you enable this setting. It uses the same SSL technology in your web browser to encrypt your username, password, and email content for POP sessions. This is usually a checkbox type setting in your email client configuration and is often labeled "This server requires a secure connection" in the advanced settings. This can be used for incoming email (POP) ONLY. SMTP over SSL is not supported.

Note: Do not confuse SSL with "Secure Password Authentication". Secure Password Authentication provides very weak encryption in comparison to SSL and is NOT supported.

Using Outlook or Outlook Express: If you use Microsoft's Outlook or Outlook Express, you can find a walk-through of the set-up procedure here:

http://www.ablehost.com/tech/docs/email_setup_outlook_express.html

Webmail

Using Webmail your users can access their email from any web browser. Newer versions of Microsoft Internet Explorer and Netscape Navigator are recommended. Other web browsers have known bugs that can affect the operation of Webmail.

Accessing Webmail

To access Webmail, open up a web browser and go to:

<http://mail.ablehost.com/webmail>

You can also access it via SSL at this location (recommended):

<https://mail.ablehost.com/webmail>

Enter your username (complete email address in the form [user@domain.com](#)) and password (defined when adding the user).

Select the POP server. IMAP is not available.

Webmail Features

The Webmail has an online help section that provides details on use of the service. Among its many features are the following:

- Address Book
- Spell Check
- Folders
- Search Messages
- Attachments
- Stored Preferences
- Multiple Identities and Sent-From addresses
- Web based Calendar
- Memo Manager
- Task List manager

Please see the help section inside Webmail for more information.

Supported Languages

Select your language when logging in. WebMail supports the following languages:

Chinese (Simplified), Chinese (traditional), Czech, Dutch, German, English (GB), English (US), Spanish, Estonian, French, Hungarian, Italian, Japanese, Korean, Netherlands, Norse, Polish, Portuguese, Russian (Windows), Russian (KOI8-R), Slovakian, Suomi, and Ukrainian

Anti-Virus Scanning

Introduction

The various desktop software solutions offered by the major suppliers, such as Symantec and McAfee, are only effective against viruses known at the time of production. Unfortunately, as many as 600 new viruses or variants emerge every month, and these products are quickly out of date unless updated every hour.

Many desktop virus scanners do provide effective protection for email. Many don't scan incoming email at all, and others don't properly scan email attachments and zip files.

The AbleServer Real-time Anti-Virus Scanning service goes on working indefinitely - 24/7/365 - because our virus definitions are kept current for you. When you opt for the virus scanning service for your Mail Server, we will defend you against threats from virus attack every minute of every day.

How It Works

As messages are relayed through the mail server, the messages and attachments are scanned for viruses. If the message contains compressed attachment file types (i.e. zip, tar, gzip, bzip2), they are uncompressed, and all of the contents are scanned for viruses. The virus scanner runs as a daemon process in the background and loads the virus definition process into memory, significantly increasing the throughput of virus scanning.

If a virus is found, the message is dropped and not delivered. A message is sent to the sender explaining why their message wasn't delivered and the virus that was found.

Anti-Virus Software

AbleServer uses Kaspersky Labs (<http://www.kaspersky.com/>) Anti-Virus for Linux Server. The Kaspersky Anti-Virus Scanner can detect: polymorphic or self-encrypting viruses, stealth-viruses, viruses for Windows 9x, Windows NT, Windows 2000, UNIX, OS/2, new Java-applet viruses, macro viruses infecting Word documents, Excel tables, PowerPoint presentations, help files, etc, Internet worms, and Trojans. The advanced heuristic analyzer is capable of detecting up to 92% of unknown viruses.

To disable Anti-Virus Scanning for a domain, change that domain's MX record to:

mx-noscan.ablehost.com

SPAM Filtering

Introduction

SPAM is used to describe the volume of Unsolicited Commercial Email (UCE) found in most mailboxes on the Internet. People that send UCE compile lists of email addresses to send advertisements to everyone they can. They can get your address in many different ways. For example, if you have your email address on your website, it can be picked up by "email harvesting robots" that search the web looking for email addresses on web pages. Some companies also sell their customer's email addresses to spammers.

Filter Common SPAM Activity

Spammers often use detectable techniques when sending SPAM. Your Mail Server can recognize these techniques and reject the message.

Some of the techniques we use include:

- DNS check for valid mail server (MX record) of domain in senders address. This means if the email address of the sender does not have a valid mail server in the DNS system then it will be refused.
- Limits number of envelope recipients (RCP TO's) for incoming email to 50. Spammers often include hundreds of recipients on one email.
- Any email including a "%" sign in the SENDER and/or RECIPIENT address will be rejected.
- Email addresses containing the local host name, IP address, or reverse host name are rejected.

Email Content Filtering

Email content is filtered for known SPAM and virus patterns.

Attachment Filtering: Because of the high risk of viruses and other problems, we automatically return all email with any of the following attachment types: .vbs, .lnk, .scr, .wsh, .hta, .pif.

Content Filtering: There are certain keywords that when found in an email will cause the email to be returned to the sender. These include any email where the following keywords are found in the subject of the email: viagra, ADV:, XXX, EXPLICIT, TEENS, A D U L T S, ADLT:. This filtering is in addition to the Anti-SPAM Filtering described elsewhere.

SpamAssassin

SpamAssassin is the leading anti-SPAM technology available on the Internet today. And is bundled with your Mail Service. SpamAssassin works by attempting to identify SPAM using text analysis. Using its rule base, it uses a wide range of heuristic tests on mail headers and body text to identify SPAM.

SpamAssassin typically differentiates successfully between SPAM and non-SPAM in approximately 95-99% of cases, depending on the kind of mail you receive.

SpamAssassin uses the following strategies:

- **Header Analysis:** Spammers use a number of tricks to mask their identities, fool you into thinking they've sent a valid mail, or fool you into thinking you must have subscribed at some stage. SpamAssassin tries to spot these.
- **Text Analysis:** Again, SPAM mails often have a characteristic style (to put it politely), and some characteristic disclaimers and CYA text. SpamAssassin can spot these, too.
- **Profile Matching:** SpamAssassin uses a wide variety of local and network tests to identify SPAM signatures. This makes it harder for spammers to identify any one strategy that will allow their messages to get through.
- **Scoring and Tagging:** SpamAssassin works by scoring a message based on its content and headers. Matching on specific SPAM characteristics will raise the score of a message. Some characteristics even lower the score. After calculating the final score of the message, if the score is greater than 5.0, the message is tagged as SPAM so that it can be filtered by the user later using their regular email program.

SPAM email has the string "SPAM: " pre-pended to the message's subject. This allows filtering using based on the keyword "SPAM:" in the subject using any popular email client.

After scanning a special header is added to the email: X-Spam-Status:. It indicates yes if the messages was identified as SPAM. For example:

X-Spam-Status: Yes, hits=16.9 required=5.0

This would be inserted into a message's headers if it was identified as SPAM with a score of 16.9.

Acceptable Use Policy

AbleServer does not allow its Mail Services to be used in/with/for any pornographic, adult, gambling, hate group and/or illegal activities. Any use of the Mail Services for or as a part of any unsolicited mass e-mailing activity is also expressly prohibited. Any violation of this agreement may result in immediate suspension of the account.

For a full description of AbleServer's Acceptable Use Policy, please review:

http://www.ablehost.com/about/acceptable_use_policy.html

Getting Support

Changes in Service

If you need changes to your account (additional mailboxes, updating your contact information, credit card information, etc.), please contact us at:

support@ablehost.com.

You can also call us at:

810-244-9100
888-740-8326 (toll free USA only)

Technical Support

The best way to get technical support is to send email to:

support@ablehost.com

You can also call us at:

810-244-9100
888-740-8326 (toll free USA only)

Please leave a message in our Technical Support voice mail. Our on call staff will be alerted to your problem. If you need to report a system down emergency leave a message in the Emergency Tech Support voice mail. Our on call engineer will be paged and investigate the outage immediately.

Appendix

Hardware and Software Used

AbleServer's Mail Server is a completely outsourced email solution. All you do is pay one monthly fee that includes your hardware, software, support, and maintenance.

Each Mail Server used by AbleServer includes these components:

- 1.3 GHz AMD Processor
- 1024 MB PC133 SDRAM
- 40 GB 7200 RPM Seagate UDMA Hard Drive
- (30 GB usable for email storage)
- 100 Mb Fast Ethernet Network Interface
- Custom Linux Operating System

Data Center: Our Mail Servers are located in a specialized Data Center designed to support a range of Internet services. We do this with redundant power including UPS and generator, and a fault-tolerant network using multiple bandwidth providers and BGP 4 routing for redundancy. Your Mail Services are monitored 24/7 by our network operations center for continuous availability. This allows us to guarantee 99% uptime.

Protection: Your Mail Services are protected at the network layer by a state-of-the-art firewall and continually monitored for intrusion. Direct access to the Mail Server is only allowed to a small group of AbleServer engineers.

Qmail Mail Transfer Agent (MTA): Our Mail Server get their great reliability from Qmail. Qmail is one of the top 5 used SMTP mail transfer agents on the Internet. It is faster, more reliable, and more secure than any other MTA available!

Qmail was released in 1997. Since that time no security flaws have been found in the software. Other organizations that use Qmail to move some of the worlds largest email volume include: Hotmail, Address.com, Yahoo! mail, Network Solutions, Verio, Ohio State (biggest US University), Listbot, Critical Path (ISP w/ 15 million mailboxes), PayPal, Hypermart.net, Casema, Pair Networks, Topica, MyNet.com.tr, FSmal.net, and vuurwerk.nl.

With our mail server you will have mail server technology previously only available to large providers and universities.

Custom Linux Operating System: Our Linux operating environment was built from the ground up with every utility and software package designed specially for

stable and secure email service. Our engineers have designed a custom operating system using Linux Kernel 2.4.18. The Linux Kernel and C library have been secured to protect against many types of attacks including: buffer overflows, TCP/IP fingerprinting & O/S detection, and TCP syn floods.

Preventing SPAM

The best method of avoiding SPAM is to be careful who gets your email address in the first place. Here are some things you can do to avoid getting on those lists:

- Pick up at least 1 email address that you do not care about. Use this as your "throwaway" email address. When you have to give an email address to someone you are suspicious of, use this email address.
- Whenever you fill out web registration forms, surveys and so on, avoid typing in your email address. If you have to give them an email address, then consider giving them your "throwaway address". Be sure to look for a box that asks if it is OK to send similar offers or information to you. Make sure you say no.
- If you have your email address on your website, it is vulnerable to "email harvesting robots" that search the web looking for email addresses on web pages. You can prevent them from recognizing your email address by using a java script code that makes it still work, but makes it unreadable for the robots (see below).
- Beware of free drawings and contests and lottos. These are usually nothing more than strategies for collecting email addresses for use in a SPAM list.
- Request that net directories (such as WhoWhere, Four11 and Switchboard) remove your name, email address, and other personal information from their databases.
- For list subscribers: If your list administrator allows it, anyone can effectively SPAM you by issuing a simple command via email to display nearly every address on the list. Send a request to the list administrator asking him or her to shield you from such postings.
- For America Online users: delete your member profile right now. All that personal information is a spammer's dream come true.
- Never respond to anything you receive as SPAM. One of the reasons people continue to SPAM is because people reward them for their efforts. Don't encourage them.
- Whenever you get SPAM that says "if you want to be removed from our mailing list, just reply?", unless you know the company and have confidence in their credibility, do NOT respond to these. Your action will more than likely guarantee that you receive even more unwanted mail. It tells the spammer that not only is your e-mail account active, but also you read your email often. While the spammer may not send you any more e-mail, he will certainly sell your e-mail address to another spammer.
- Never forward email to large numbers of people. If you MUST send email to large numbers, then send it to them with the bcc: option so others cannot see everyone else's email address.

How To Stop Address Harvesting on Your Web Site

There are email harvesting robots that are programmed to seek out and review web pages looking for any email addresses they can find. They then take these email addresses and add them to SPAM lists.

Here is a nice Java Script you can use to hide your email addresses listed on your web pages.

```
<script language="JavaScript"><!--var name = "yourname";  
var domain = "yourcompany.com";  
document.write('<a href="mailto:' + name + '@' + domain + '">');  
document.write(name + '@' + domain + '</a>');  
// --></script>
```