

Third Party Mail Relay Blocking

The following provide some suggestions on how to secure your current mail system against third party relaying. Find your mail client from the listing below for details:

Note: This information is merely a starting point. We recommend to all customers that you follow-up with the software vendor for further information, since we do not support any of these programs.

Sendmail Version 5

Unfortunately, you are running an outdated mailer. There is no known solution to prevent relay. Moreover, the mailer has security holes. Your mail system is a security risk; you should strongly consider upgrading to a modern mailer.

Sendmail Version 8

Starting with version 8.9.0, Sendmail prohibits relay by default, as well as providing a number of parameters to control this feature. See the Anti-Spam Configuration Control section of the cf/README file for information on these settings.

Rulesets for version 8.8.x are available via Claus Abmann's web site at sendmail.org. Many sites which run 8.8.x have added anti-relay configuration, but are still susceptible to the "percent hack." Please pay special attention to the `removelocal` portion of `check_rcpt` in Claus's recipes to fix that.

Another approach is to limit mail server access to only those users who have authenticated themselves with a POP password. This is the so-called POP-before-SMTP solution. Although this is more complicated to setup, it is an excellent solution for providers that have "roaming users." ISP's that are members of the iPass network should email ask@ipass.com to obtain the "Anti-Spam Kit" for Sendmail 8.8.

Caution: Most of these solutions require you to setup a list of domains to which relay is allowed. Be sure to include all authorized domains in this list. Don't forget downstream domains for which you MX, as well as virtual domains that you serve. Otherwise you will begin rejecting mail that should not be rejected.

For more information, please refer to www.sendmail.com.

Eudora WorldMail Server

As delivered, WorldMail Server version 1.0 is vulnerable to relay. The fix you must obtain the Connection Management Center (CMC) utility to secure your WorldMail Server against unauthorized relay. You can download a copy for free. The manual describes this feature starting on page 9, "Restricting Access to Specific Services Based on IP Address".

Select "SMTP Relay (Non-Local Only)" as the access control to configure. Check off "Denied Access" as the default setting. List the IP address of the hosts and networks that should be allowed to relay mail through your server. For more information, please refer to <http://www.qualcomm.com>.

Third Party Mail Relay Blocking (cont'd)

Microsoft Exchange Server

The Exchange Server Internet Mail Service allows you to configure the server to allow mail relaying. This allows ALL mail to be routed if the functionality has been enabled in the Internet Mail Service 'Routing' property page. Exchange Server 5.5 Service Pack 1 allows the administrator to impose restrictions on routing. To enable these restrictions on routing functionality, perform the following steps:

- Install Exchange Server 5.5 Server Pack 1 (or greater).
- Open properties on Exchange Server Internet Mail Service. Select the 'Routing' page.
- After SP1 installation, select Routing Restrictions.
- Click Routing Restrictions to bring up a dialog box with additional Restrictions.

Groupwise

GroupWise 5 GroupWise Internet Agent (GWIA) may be secured against unauthorized relay:

- Using NWAdmin, go to the details page of the Gateway.
- Click on the "Access Control" tab.
- Click on the "SMTP Relay" button.
- Check the "Prevent Message Relaying" radio button
- Click OK.

There is a workaround to secure the GroupWise SMTP/MIME gateway:

- Edit the DOMAIN/WPGATE/SMTP/GWSMTP.CFG file (with any text editor)
- Add the switch "/NOROUTING". Mail relay will now be disabled.
- If you have the option set to save problem mail, the messages instead will be saved into your problem directory, so be sure to keep an eye on it.

In version 5.5, add "/NOROUTING" to the GWIA.CFG file in the SYS:SYSTEM folder.

Mercury

The Mercury mailer is an NLM for Novell servers. Preventative measures blocking unauthorized relay have been added as of version 1.40. The Mercury/32 mailer is re-designed for Windows 95 and Windows NT. Preventative measures blocking unauthorized relay have been added as of version 2.11. To disable relaying, the following text should be added to the [MercuryS] section of mercury.ini":

```
[MercuryS]
Relay : 0
Strict_Relay : 1
Allow : 2.3.4.5 # The offsite backup (MX server)
Allow : 192.168.XXX.0 # Our local network
Allow : 192.168.YYY.5 # A single other machine we allow
```

The "allow/refuse" entries under [MercuryS] must end with the line:

```
Refuse: 0.0.0.0
```

Third Party Mail Relay Blocking (cont'd)

Message Exchange (MX)

All information indicates that version 4.2 has no relay control features. Version 5.0 and above, however, have these features. For version 5.1, full details are provided in the file mx_root:[doc]MX_MGMT_GUIDE.TXT. Briefly, it's:

```
MCP SET SMTP/NORELAY
MCP RESET SMTP_SERVER
```

NTMail

NTMail provides several anti-relay and anti-spam measures, including some add-on options.

- Recent versions of NTMail leave relaying turned off by default. Information on selectively allowing authorized relay is available [here](#).
- For older versions, secure against unauthorized relay by selecting the "Only Accept Local Mail" option.

Enter the hosts that are allowed to relay mail through your server in the "Treat as Local" section. You can specify either domain names or host IP addresses. Use addresses if you can as names may be subject to spoofing.

Lotus Notes and Lotus Domino

To disable relaying, insert the following into the notes.ini file:

```
SMTPMTA_REJECT_RELAYS=1
```

Two more notes.ini settings which may help:

```
SMTPMTA_DENIED_DOMAINS
```

The NOTES.INI variable (SMTPMTA_DENIED_DOMAINS) allows you to enter the pathname of an ASCII file containing domains that your organization wants to prevent from sending mail. If it is NULL or not present, the MTA will accept mail promiscuously.

```
SMTPMTA_HELO_DOMAIN_VERIFY
```

A NOTES.INI variable (SMTPMTA_HELO_DOMAIN_VERIFY) authenticates the domain name specified in the HELO/EHLO console command. It does this by verifying that the IP address used by a remote host is actually associated with the purported Domain Name that the host has supplied.

Note: the Helo Verify and Denied Domain Lists features may be used together or independently of each other.

Click [here](#) for a full list of ini file settings. Other anti-spam settings that Notes supports are described in www.keysolutions.com. For the main Lotus site, please refer to: www.lotus.com.

Third Party Mail Relay Blocking (cont'd)

QuickMail Pro Mac 1.1.1r1 Server

Servers that support mail relaying can accept and deliver incoming messages intended for non-local addresses. This capability can be extremely valuable if you want one server to distribute mail for many people from various domains. It can also be a drawback due to the unsolicited bulk E-mail (spam) that often overloads Internet servers.

QuickMail Pro Server has controls that can reduce the amount of mail routed through your server so your LAN users have the fastest mail possible. To reduce mail flow on your Internet mail server:

- Select Domain Setup in the Configure menu.
- Double-click the SMTP domain entry in the Domain Setup window.
- Select your mail relay options in the Relaying box of the SMTP Domain dialog
- Click OK.

For more information, please refer to: www.cesoft.com.

Appleshare IP Server (ASIP)

Information on how to secure the Appleshare IP Server against mail relaying can be found at the above link.

For more information, please refer to:

<http://til.info.apple.com/techinfo.nsf/artnum/n31108>

For more information on relay blocking in general, or if the mail client you use isn't referenced on this website, please refer to Anti-Relay: Stop Third-Party Mail Relay.