

Controlling SMTP Relaying with Microsoft Exchange

Topics on this Page

- [▼What Is Relaying?](#)
- [▼Why You Should Care](#)
- [▼What to Do About It](#)
- [▼Where to Learn More](#)

By Paul Robichaux

What Is Relaying?

If you've ever received unwanted spam in your mailbox, then you already know what relaying is: using a server to accept and then resend mail to recipients on another server. In the simplest case, *alice@a.com* connects to the SMTP server at *b.com* and uses it to deliver a message to *charlie@c.com*. Note that this isn't the same as when Alice uses her own organization's SMTP server. A more practical example: say you're on the road with your laptop. You'll probably have a dial-up (or maybe broadband) connection that will assign you an IP address outside your normal network block. If your SMTP server accepts messages from you for delivery to third parties (e.g. addressees not on your own mail server), that's relaying; a server that has relaying turned on will accept mail for recipients in other domains, then attempt to redeliver it.

Why You Should Care

In some cases, relaying is desirable, like when you're traveling and want to use your regular Exchange server as an SMTP host. However, it's important to couple relaying with restrictions and authentication; if you don't, spammers will be able to use your relay to send out spam messages—you'll get the blame, because the messages will appear to have originated from your server! Apart from the community benefit of helping to stop spam, configuring your Exchange server's relay settings properly offers the benefit that it keeps you from being a spam injection point, saving you bandwidth and lots of potential hassles.

What to Do About It

There are separate configuration processes for Exchange 5.5 and Exchange 2000. In both cases, you'll be configuring the component that handles Internet mail to reject mail addressed to non-local recipients; there are some additional settings you can tweak to allow relaying with authentication or from particular IP addresses. Bear in mind that if your Exchange server is providing SMTP service to POP3 or IMAP4 clients, you'll have to turn on relaying in some fashion.

Blocking relaying in Exchange 2000

Exchange 2000 has a very flexible set of anti-relaying features built in. You configure them at the SMTP virtual server level, so that you can set different relaying properties on different servers. One common use for this is in setting up two virtual server: one with relaying disabled on port 25 for standard traffic, and another with authentication-based relaying turned on on a non-standard port number. Your remote clients can configure their mail clients to use the non-standard port; this approach neatly avoids the problem of spammers who scan for open relays.

The actual process of controlling relays is simple, but it varies slightly depending on whether you want to configure relaying for the SMTP virtual server or an SMTP connector. (If you don't know the difference between virtual servers and connectors, check out the Microsoft Knowledge Base article [Q294736](#) .) Connector relay controls are outside the scope of this article; check out the "Where to Learn More" section below for more details.

Controlling SMTP virtual server relaying

1. Launch Exchange System Manager. Navigate to your SMTP virtual server (it's under Administrative Groups | *yourAdminGroup* | *yourServerName* | Protocols).
2. Right-click the virtual server and choose the Properties command.
3. Select the Access tab.
4. To restrict inbound SMTP connections to a particular address range (for example, if your POP3/IMAP4 clients are using a block of addresses via a VPN or dial-up connection), use the Connection... button to specify which addresses may make SMTP connections. Note that the settings in the Connection dialog apply to all hosts that try to use this SMTP server.

To control SMTP relaying, click the Relaying button. In the Relay Restrictions dialog box (see Figure 1), you can do the following:

- ☒ To turn off all relaying from everywhere, select the "Only the list below" radio button, then leave the Computers list blank. This is the default setting.
- ☒ To allow relaying from a single computer or block of network addresses, use the Add button (see Figure 2) to add the IP addresses or blocks that you want to be able to relay. You can also allow relaying by domain name instead of IP address, although there is a performance penalty if you do.
- ☒ To block a specific set of IP addresses, select the "All except the list below" radio button, then use the Add button to add the specific computers or network addresses that you want to be able to relay.
- ☒ To allow computers that authenticate to Exchange to relay, no matter what other restrictions are in place, make sure that the "Allow all computers which successfully authenticate..." checkbox is turned on.

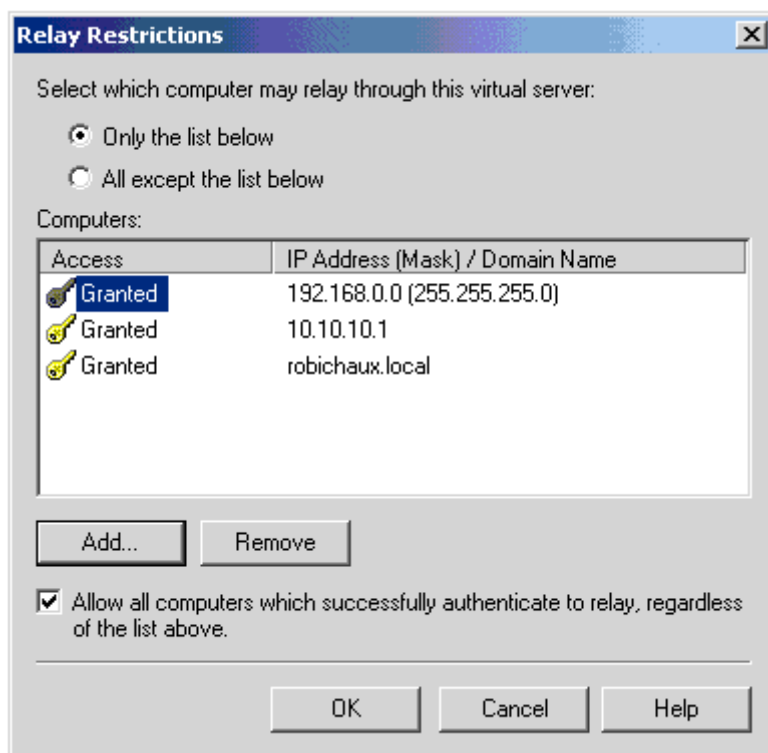


Figure 1 Relay Restrictions

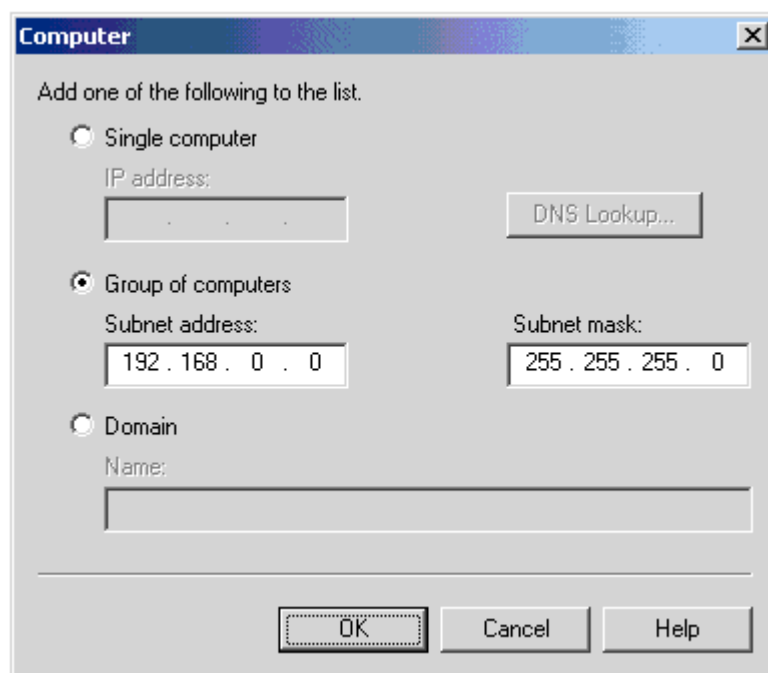


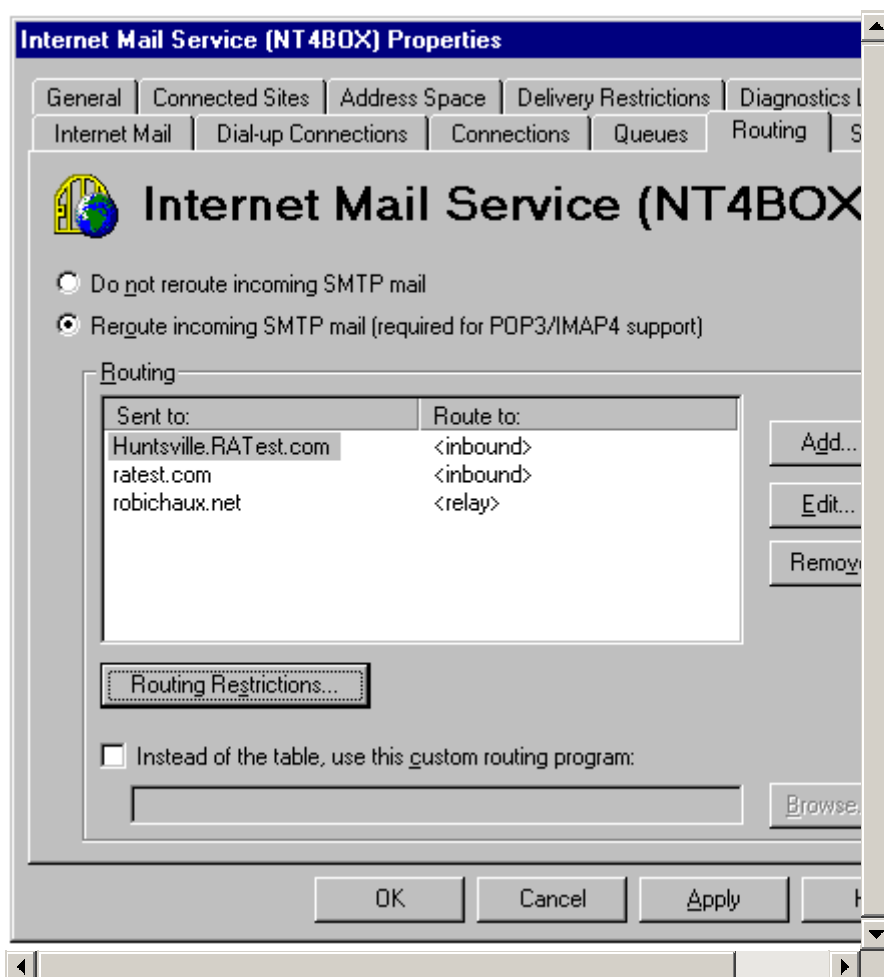
Figure 2 Add to allow relay

Blocking relaying from in 5.5

First things first: Exchange 5.5 added relay control features to the IMS interface in SP1. Of course, you should be running the latest service pack, but if you're not, [go get it](#) and install it before proceeding with these instructions—each service pack

includes security fixes that you'll want to have on any Internet-exposed server. (If for some bizarre reason you can't upgrade to SP1 or later, see the Microsoft Knowledge Base article [Q193922](#) for help on configuring the IMS relay subsystem manually.)

When you install the IMS, Exchange Administrator will ask you if you want to enable relaying or not; the default setting turns it off. After installation, you control relaying in Exchange 5.5 via the Routing tab (see Figure 3) of the Internet Mail Service Properties dialog. Note that changing any of the relaying-related settings will require you to stop and restart the IMS before they take effect.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 3 Routing Tab of Internet Mail Service Properties

To turn off relaying completely

If you want to prohibit any SMTP relaying at all, make sure that the "Do not reroute incoming SMTP mail" radio button is selected. That's easy enough! You should probably have this turned on for servers inside your firewall that don't normally accept connections from outside clients.

To allow some kinds of relaying

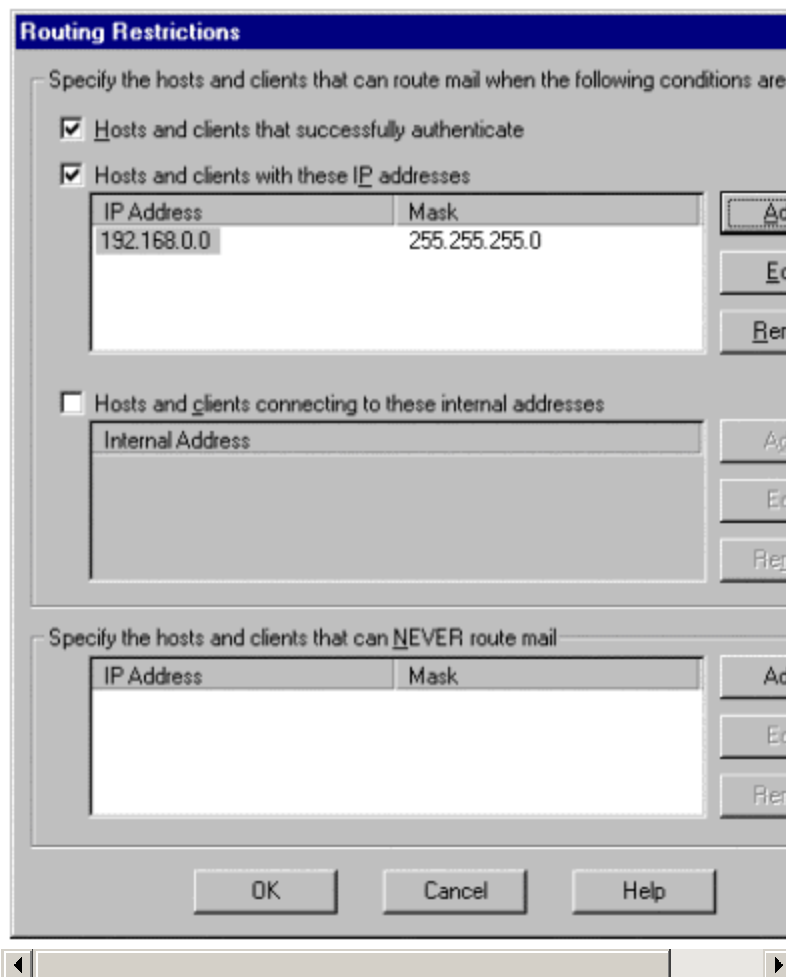
First, you have to turn on relaying by selecting the "Reroute incoming SMTP mail

(required for POP3/IMAP4 support)" radio button. Once you've done that, there are two primary mechanisms for controlling relaying:

- ✎ The Routing list shows which domains your server will accept SMTP mail for. In the example, *ratest.com* and *huntsville.ratest.com* are listed as inbound, meaning that the IMS will accept mail and attempt to deliver it locally. The *robichaux.net* domain is explicitly listed as a relay domain; that means that it was manually added (using the Add... button) as a domain for which I want to accept SMTP mail, no matter what.
- ✎ The Add..., Edit..., and Remove buttons let you change which domains appear in the Routing list, as well as what the IMS will do with mail for those domains: block it, accept it for relaying, or treat it as inbound mail.

The Routing Restrictions button (see Figure 4) is where you can do what most administrators want to do: allow legitimate clients to relay while blocking spammers. By default, all of the controls in this dialog are turned off; you'll have to set the specific restrictions you want to enforce.

- ✎ If you want any client who logs on (e.g. for POP3 or IMAP4 access) to be able to relay, check the "Hosts and clients that successfully authenticate" checkbox. Note that by requiring SMTP authentication in conjunction with this option, you can allow SMTP servers—not just clients—to relay through your server.
- ✎ To allow specified IP addresses—internal or external—to relay, check the "Hosts and clients with these IP addresses" checkbox, then use the Add, Edit, and Remove buttons to build the list of IP addresses from which you want to accept relay traffic. Remember that this checkbox controls relaying when you have selected the radio dial for "Reroute incoming SMTP ..." in the Routing tab. You should normally check this box; doing so will prevent relaying. If you leave it unchecked, your server is open for relay.
- ✎ If you want to allow relaying only from clients that connect to a particular IP address on your server, check the "Hosts and clients connecting to these internal addresses" checkbox.
- ✎ To stop a particular group of hosts or clients from *ever* relaying mail, put their IP addresses and netmasks in the "Specify the hosts and clients that can NEVER route mail" list.



If your browser does not support inline frames, [click here](#) to view on a separate page.

Figure 4 Restricting certain hosts and clients

Where to Learn More

- ✂ You can check your servers to see if they're open relays by using a tool like [Sam Spade](#) (discussed in an article in [Information Security Magazine](#)). Some other tools are mentioned in Microsoft Knowledge Base article [Q249266](#) .
- ✂ Microsoft Knowledge Base KB article [Q260973](#) discusses the fine points of setting up SMTP connectors to allow mail relaying by domain, instead of by client address.
- ✂ If you're not sure whether to use an SMTP virtual server or SMTP connector, Microsoft Knowledge Base KB article [Q265293](#) may help clear things up.
- ✂ If you actually *want* to set up a relay host, you can. For example, you might need to do this if you have a single set of SMTP gateway servers that internal hosts need to pass message traffic to. Be careful, and refer to Microsoft Knowledge Base article [Q293800](#) before you do so.
- ✂ The [Internet Mail Consortium](#) has a fascinating [report of some experiments](#) they did to see how many relay hosts there are on the Internet.

Paul Robichaux is the principal of Robichaux & Associates, Inc, which provides

programming, technical communications, and security services to customers ranging in size from local auto dealerships to Microsoft. He's glad to have his latest book [Managing Microsoft Exchange Server](#) (O'Reilly & Associates) on the shelves so he can spend more time with his family. He welcomes reader questions at security@robichaux.net.

We at Microsoft Corporation hope that the information in this work is valuable to you. Your use of the information contained in this work, however, is at your sole risk. All information in this work is provided "as -is", without any warranty, whether express or implied, of its accuracy, completeness, fitness for a particular purpose, title or non-infringement, and none of the third-party products or information mentioned in the work are authored, recommended, supported or guaranteed by Microsoft Corporation. Microsoft Corporation shall not be liable for any damages you may sustain by using this information, whether direct, indirect, special, incidental or consequential, even if it has been advised of the possibility of such damages. All prices for products mentioned in this document are subject to change without notice.

[Contact Us](#) | [E-mail this Page](#) | [TechNet Newsletter](#)

© 2003 Microsoft Corporation. All rights reserved. [Terms of Use](#) [Privacy Statement](#) [Accessibility](#)