

Spam, more correctly called unsolicited bulk email (UBE) or unsolicited commercial email (UCE), is a real concern to system administrators and users today. While nothing will completely eliminate spam, there are several things that you can do to minimize this electronic plague.

An Overview of Spam Control

What does `sendmail` have to help you fight spam? The following features of `sendmail` help you combat unwanted email.

- Access Database
You can use the access database to block email based on the user name portion of the address, the domain part of the address, or the full address.
- Relay Access Control
Use the relay access options to control who can pass mail through your system, and how your system handles mail.
- Blocking Senders
By utilizing the Realtime Blackhole List and other databases of recognized spammers, you can prevent some offending email from passing through your system. In addition, your `sendmail` configuration, by default, rejects mail with MAIL FROM: parameters

that indicate potential spamming activity. (Though not recommended, this chapter includes steps for changing the default setting of these parameters.)

- **Delay Checks**

The Delay Checks option can alert `postmaster` or another system administrator to potential spamming activity.

This chapter also covers how to blacklist recipients—that is, deny incoming mail for specific recipients. The Blacklist Recipients option cannot be enabled unless you have set the access database.

Which features you choose—and how you implement them—depends on your system and users.

Using an Access Database

Your first line of defense against spam could well be the access database. This database lets you reject mail from specific domains, hosts, or even mail accounts.

Once enabled, the access database lets you include entries for rejecting and relaying mail from specific users, hosts, and domains. Unfortunately, some spammers may get around these access database settings by forging valid addresses, but you can limit the majority of problems here.

Enabling an Access Database

Enable the access database, and then create database entries in order for `sendmail` to take advantage of the access database.

To enable the access database, follow these steps:

1. **On the Advanced Configuration page, select Spam Control on the options menu.**

A Spam Control page appears.

2. **Under the Access Database option, choose Yes, with optional value.**

The default path is included in the text field. Accept the default, or type in a new file name.

You can also enable Accept Unqualified Senders and Accept Unqualified Domains on this page.

3. Select Edit Map.

The Create a New Map page appears.

If the access database does not exist, you will see a message informing you of this. Select OK to continue. The Sendmail Administration Console (Admin Console) creates the new access database.

Now you must create your database entries. Proceed to the next section, “Configuring an Access Database” on page 145.

Configuring an Access Database

To create access database entries:

1. **Move the cursor to the text field under KEY. Type the domain name, host name, IP address, or user name to be modified.**

If entering a user name, you must include the trailing at sign (@) to signify that only the user name portion of the address should be checked.

You can also use prefixes to modify the entry further. See the Access Database online help page for more detailed information about the access database editor.

2. **Move to the MAPPING text field (on the right) and type the action to be taken when a lookup finds this entry.**

Table 11-1 shows the valid choices.

Table 11-1 Access Database Relaying and Blocking Options

Entry	Description
OK	Accept email even if other rules in the current rule set would reject it
RELAY	Allow domain to relay through your server
REJECT	Reject sender/recipient with a message
DISCARD	Discard the message
nnn text	An RFC822 error code in the 400 or 500 series, followed by message text
Error: nnn: text	Any error
Error:D.N.S.: nnn text	An RFC1893 compliant error message, followed by message text

3. Select the Insert button to insert your new entry.

You can also type entry data directly into an open map line.

4. Repeat this process for all desired entries, then select Save to save your map changes.

No changes or new entries are saved to the access database until Save is selected.

For example, to reject all mail coming from the domain `spammer.pogonip.net` and send a message to the sender explaining that spam is not accepted by your system, you would enter the following into the access database:

```
SPAMMER.POGONIP.NET          550 Spam not accepted
```

If you wanted to simply reject messages from this domain, you would create the entry:

```
SPAMMER.POGONIP.NET          REJECT
```

For more detailed information about the access database and anti-spam settings, see the online help.

Relay Access Control

In the earlier days of email, indiscriminate messaging was commonplace. Now, however, most MTAs include settings that restrict relaying to authorized parties only.

Transmission of messages from one site outside your domain to another site outside your domain is called relaying. PRODUCT X's default is not to allow relaying.

The relay control features are among the most useful tools in fighting spam.

By default, `sendmail` does not allow relaying. However, you may allow other systems to use your mail server. Use the Relay Access features to limit access to systems that you choose.

There are two types of relaying:

- Incoming, in which mail from anywhere is relayed to recipients within an authorized system.
- Outgoing, in which mail from an authorized system using a recipient address matching a list of authorized systems is relayed.

There are several relay-related features available to you in PRODUCT X. A list of these features, along with their general use, is shown in Table 11-2.

Table 11-2 Relaying Features

Use this Option	To
Relay Domain	Allow specified domains to relay
RELAY_DOMAIN_FILE() (Expert Configuration only)	Specified file name contains a list of domains allowed to relay
Relay Entire Domain	Allow any host in any of your local domains to accept mail either to or from any other host in your domain

Blocking Senders

Table 11-2 *Relaying Features*

Use this Option	To
Relay Based on MX	Allow relaying based on the MX records of the host portion of an incoming recipient address
Relay Based on Envelope From:	Relay if the sender specifies a return path domain that is a local domain
FEATURE(relay_mail_from) (Expert Configuration only)	Relay if the mail sender is listed as RELAY in the access map
Loose Relay Check	Prevent the address from being stripped down

You can learn more about these features in the sections covering relays in Chapter 5, “Configuring a Network Mail System.”

Blocking Senders

Blocking senders provides a simple, straightforward way to make sure that messages from some addresses are automatically rejected by your system. This method ensures that mail from certain addresses, user names, domains, or IP addresses is rejected categorically; the messages never get a chance to be relayed through your system.

DNS Blackhole Lists

A DNS Blackhole List is a rejection list of spammers maintained in a DNS database. Selecting this option causes `sendmail` to reject mail from any site found on the DNS Blackhole List server.

Once activated, you may optionally include a rejection message to send to the originator.

If you do not specify a host name as an optional argument, `sendmail` will check the Realtime Blackhole List site maintained by the MAPS project: `rbl.maps.vix.com`. In cases where multiple DNS servers are used, each is checked in turn.

To turn on DNS Blackhole blacklisting and add additional DNS servers, perform these steps:

1. From the Advanced Configuration menu, choose Spam Control > Blacklisting.

A page with both blacklisting features appears.

2. If you want to block incoming mail for users specified in the access database, select the Yes radio button.

3. If you want to add any servers to the DNS blackhole list, select Add to change the page to allow additional DNS servers; if not, skip to step 5.

The page changes to show the DNS Server and Optional Rejection Message text fields.

4. Enter the DNS server to include and optionally a text message to send with the rejection notice.

By default, `rbl.maps.vix.com` is added. You can choose to add an optional text message or not.

Customizing the rejection text message can be a good way to “tag” the DNS server on which the spammer was found. Enter the server name, any other text message to be sent, or both.

For multiple DNS server entries with or without an associated rejection message, enter the appropriate information into the text field and select the Add button.

5. Select the Apply button, and then save your changes using the Save button.

Accepting Unqualified MAIL FROM: Senders

By default, `sendmail` refuses mail if the MAIL FROM: parameter has an unresolvable domain or if the parameter is an unqualified domain. (MAIL FROM: is an SMTP command that specifies a message is to follow.) This is the safest way to operate. It makes it more difficult for spammers to pass mail through your system.

In most cases, you should leave the default settings as they are.

Accept Unresolvable Domains

If you want to accept domains when the `MAIL FROM:` parameter cannot be located in the host name (DNS) service, you should enable the Accept Unresolvable Domains feature. This is not recommended for normal use, but in some cases may be necessary. For example, you may want to enable this option if your system is inside a firewall that has only a limited view of the Internet host name space.

Note – You will not be able to return mail to the sender unless you have a “smart host” forwarder.

To allow `sendmail` to accept unresolvable domains:

1. In the Advanced Configuration page, choose Spam Control on the options menu.
2. By the Accept Unresolvable Domains feature, change the default No setting to Yes.
3. Apply and Save your changes.

Accept Unqualified Senders

Also, the default `sendmail` settings reject mail if the `MAIL FROM:` parameter does not contain a domain as well as a user—for example, `MAIL FROM: <joe>`. If you want to continue to accept such senders, enable the Accept Unqualified Senders feature.

To enable `sendmail` to accept unqualified senders:

1. In the Advanced Configuration page, choose Spam Control on the options menu.
2. By the Accept Unqualified Senders feature, change the default No setting to Yes.

3. **Apply and Save your changes.**

Blacklisting Recipients

The Blacklist Recipients option uses access database entries to deny—or blacklist—incoming mail for certain recipient users, host names, or addresses.

If these lines are added to the access database and the Blacklist Recipients option is enabled, mail is rejected for these targets. Since this option depends on whether the Access Database option has been set, make sure that you have enabled the access database before attempting to use the Blacklist Recipients option.

To enable the blacklisting option:

1. **In the Advanced Configuration page, choose Spam Control > Blacklisting.**
A page with both blacklisting features appears.
2. **By the Blacklist Recipients option, select the Yes radio button.**
3. **Select the Apply button.**
4. **Save your changes.**

Even though you have now enabled the Blacklist Recipients feature, you must enter the recipient information into the access database. See “Using an Access Database” on page 144 for details.

Delay Checks

By using the Delay Checks feature, you can change the order in which mail checking rule sets are applied. The recipient is now the first check performed, essentially bypassing the relay and mail rule sets. This feature can ensure that certain types of recipients are always reached (for example, `postmaster`, a complaint handler, or a tech support address). This allows you to set parameters that specify the addresses for which this order applies.

When parameters are applied, `sendmail` calls the rule sets in this reverse order when two conditions exist: the access database is configured and recipient name addresses contain an access map left-hand side `To:` tag entry and matching right-hand side entry of `SPAMFRIEND` or `SPAMHATER`. These are the only two optional parameters used with Delay Checks.

First, the recipient address is looked up in the access database. It examines left-hand side access database entries containing “`To:`”.

- If the argument specified is `friend` and the recipient is found and has an access map right-hand side entry `SPAMFRIEND`, then the rule sets `check_mail` and `check_relay` are skipped.
- If the argument specified is `hater` and the recipient is found and has an access map right-hand side entry `SPAMHATER`, then the rule sets `check_mail` and `check_relay` are applied.

For example, by setting the argument to `friend` and including the following access map entry:

```
To:abuse@          SPAMFRIEND
```

normally rejected spam email to `abuse@localdomain` will get through.

To enable the delay-checking feature:

- 1. From the main menu, select the Edit Existing Configuration option.**

If your configurations are on more than one cluster or host, the Select Host or Cluster page appears (follow instructions in step Step 2). If you have only one host or cluster, the Admin Console goes directly to the Load Configuration page (skip Step 2).

- 2. If necessary, select the host or cluster to configure and choose the Select button.**

- 3. Highlight an existing configuration or type a configuration in the text field and choose the Load button.**

The Advanced Configuration page appears.

- 4. Select Expert Configuration from the left-side options menu.**

The Expert Configuration page appears.

5. Select `FEATURE(delay_checks)` from the list box, and then select the **View/Edit** button.

The page changes to allow you to enable the Delay Checks feature.

6. Select the **Yes, with Optional Value** radio button.

If you want to use the `friend` or `hater` values, enter one in the text field. You can then use the access database to limit the recipients for which the reversed order applies. If you enter no values, the reversed checking order applies to all recipients.

7. Select **Apply**, and then save your changes using the **Save** button.

Allowing Anyone to Relay

By default, the `sendmail` configuration files do not permit accepting mail from outside your domain and sending it to another host outside your domain. While *not recommended* in most cases, PRODUCT X does provide a method to override this option: Promiscuous Relay. This option sets your site to allow mail relaying from any site to any site.

To ignore the recommended settings and enable the Promiscuous Relay feature, perform the following steps:

1. On the options menu of an **Advanced Configuration** page, choose **Spam Control > Relay Access Control**.

The Relay Access Control page appears.

2. By the **Promiscuous Relay** option (near the bottom of the page), select the **Yes** radio button.
3. Select **Apply**, and then save your changes using the **Save** button on the control bar.

