

Email Security Service Quick Reference Card

Basic Security Tips

Add All Domains

Add all domains and subdomains to the email protection service. For domains that share the same users lists, set up domain aliases. Update your MX records for each domain and domain alias.

Limit SMTP (port 25) Traffic

After you add all of your domains, limit SMTP (port 25) traffic at the firewall to only allow connections from email security service IP addresses. This prevents spammers from delivering spam directly to your server.

Enable Blatant Spam Blocking

Blatant Spam Blocking minimizes the number of obvious spam messages in your user quarantines.

Add Users and Mailing Lists

Add all users and their aliases, and mailing lists. You can upload a list of users using batch commands or through automated methods such as Directory Sync or SmartCreate. After adding all of your users, consider turn on Non-Account Bouncing to block messages sent to invalid addresses.

Set Up Virus Protection

Enable Non-Account Virus Blocking for your domains so that virus-infected messages sent to unregistered users are automatically deleted. Also configure Attachment Manager to block or quarantine messages with attached executable files, which can contain hidden viruses.

Enable Connection Manager Blocking

When Connection Manager detects attacks, it automatically protects your server. You can also block specific IP ranges and designate trusted servers that will not be blocked as attackers.

Configure Alerts and Notifications

Configure your Delivery Manager and Spooling Manager administrator alerts to track critical mail server events.

Set Up Disaster Recovery

If you have the optional email spooling feature, set up Spool Manager for disaster recovery.

Create an Emergency Plan

For mail flow issues, develop an emergency plan and familiarize yourself with your support options and troubleshooting procedures.

Email Security Service IP Ranges

Note, for system 20 customers, both sets of IP ranges are applicable.

| System | IP Range | CIDR Range | IP/Subnet Mask |
|----------------|------------------------------------|------------------|--|
| 5, 6, 7, 8, 20 | 64.18.0.0 – 64.18.15.255 | 64.18.0.0/20 | 64.18.0.0 mask 255.255.240.0 |
| 20, 200, 201 | 207.126.144.0 – 207.126.159.255 | 207.126.144.0/20 | 207.126.144.0 mask 255.255.240.0 |

Your system is shown the URL when you log in to the Administration Console. The system number is prefaced by “ac-s”.

Technical Support Resources

Log in to the Support Portal to view the current system status, search the knowledge base, get the latest training and documentation information, and submit or check the status of a support case. Log in at:

<http://support.postini.com>

You can also find out news and share tips and best practices with other users at the Community Forum:

<http://community.postini.com>

During a Spam Outbreak

Occasionally there may be a large-scale spam outbreak across the Internet. The email security service blocks nearly all spam messages. However, with spammers launching mass mailings with new attack methods, you may temporarily see a few similar spam messages in your inbox.

Please be assured that the email security service is addressing the issue and updating filters to protect against the attack. For the status on spam outbreak, please check the Support site.

Troubleshoot Spam for a User

If you find a spam messages delivered to a particular user, please follow these steps to troubleshoot:

Has the user address been added to the email protection service?

Search for the user's address in the Administration Console. If not found, then the mail is being delivered without filtering. Add the user address, and note:

- ◆ If the address is associated with user who's already registered, add a user alias.
- ◆ If the service could recognize the address via domain aliasing, create a domain alias for the user's domain.
- ◆ If the address could be a distribution list, see the distribution list solution below.

Was the message sent to a mailing or distribution list rather than an individual user?

Find the message header's To address, and search for that address in the Administration Console. If the address is not there, you must add the mailing list. Since mailing lists tend to include those outside of your organization, do not add the list as a user. Add it as an alias of the responsible owner so that the Quarantine Summary and password messages are sent to the mailing list owner rather than the entire mailing list itself.

Was the message sent directly to your mail server bypassing the protection service?

Remember, spammers don't follow DNS standards for selecting MX records. To prevent bypassing of the email protection service filters, set up your email server or firewall to only accept email from the protection service's IP ranges (found on the reverse side).

Was the sender's address in the Approved Senders list?

If the sender or sender's domain is on an Approved Senders list, either the user's personal list or a list defined for the user's org, messages will be delivered, regardless of spam-like content. This is also true if the spammer has spoofed the sender address to match an Approved Sender.

Review the user- and org-level Senders Lists and delete any large and well-known domains that are often spoofed by spammers.

Have users added their own addresses or domains as an Approved Mailing List?

- ◆ If so, all spam addressed to the user, regardless of spam settings, will be delivered to that user's inbox.
- ◆ In the Administration Console, remove the user's address or domain from user's Approved Senders and Recipients lists.

Did a user within your organization send the message?

Messages exchanged among users on the same server aren't processed by the email protection service, unless you configure your server for intradomain filtering. Review the message headers to see if the email was sent from someone within your organization.

Was the mail delivered from quarantine?

The user or an administrator may have delivered the message from Quarantine.