

## **Title: What If I've Reached the SMTP Limit on my Virtual Dedicated/Dedicated Server?**

### **Subtitle: Virtual Dedicated Linux**

Author: Jane83

Date: 2008/2/26

URL: <http://www.powerhoster.com/domainhosting/modules/article/view.article.php/c8/1242>

Keywords: the SMTP Limit

There is a daily limit of 1,000 outbound emails from your dedicated/virtual dedicated server. There are several other reasons besides "standard email" that can cause you to reach this daily restriction. The following are a few things you can check: [Verify That Your Domain Name is Not Sending Out Bouncebacks](#). The default Plesk setting is to bounce email sent to non-existent users. This means that if your domain is coolexample.com, and someone sends an email to a non-existent user (ex: var id='johndoe';var host1='coolexample.com';var host2='';document.write(""+id+'@'+host1+'.'+host2+'');), it is defaulted to send a message back saying "This user does not exist". If your domain receives a lot of incoming mail to non-existent users, the daily limit can be hit in no time. The solution is to modify your mail preferences to reject mail sent to non-existent users. To reject mail sent to non-existent users in Plesk: From the Plesk control panel click Domains. Click Select Domain, then click Mail. Click Preferences and then click the Reject radio button, and click OK. NOTE: You will need to do this for all domains on the server. [Test Your Server for an Open Relay](#). An open mail relay is a SMTP server that is configured in such a way that it allows anyone on the Internet to send email through it. You can use the tool at <http://www.abuse.net/relay.html> to test for an open relay. To close an open relay: Plesk:

On a Linux server with Plesk, you will want to log into Plesk as the admin account and click Server > Mail. Make sure that you have either chosen Closed or Authentication Required next to the Relay option. cPanel:

Servers with cPanel are configured as closed relays by default. If you suspect there is an open relay configured, you can run the following commands using SSH:

```
/scripts/fixrelayd
```

```
/etc/rc.d/init.d/antirelayd restart
```

```
service exim restart Consult the Email Logs & Mail Utilities on Your Server. NOTE: For Plesk
```

(Linux), cPanel, & Simple Control Panel, you will want to use SSH as your main means of

troubleshooting. If you do not have an SSH client, you can download Putty free [here](#). For Plesk

(Windows), you will want to log into the server using Remote Desktop. For more information on

accessing your sever with Remote Desktop see [Accessing Your Windows Dedicated Server using Remote Desktop Connection](#)

Plesk/Linux Servers:

```
/usr/local/psa/var/log/maillog (Qmail log)
```

```
/var/qmail/bin/qmail-qstat (View the amount of messages currently in your outbound queue)
```

```
/var/qmail/bin/qmail-qread (List out all messages in your outbound queue)
```

```
find /var/qmail/queue -name XXXX | xargs cat | less (Read the entire contents of an email, including headers, where XXXX is the ~8 digit ID specified on the /var/qmail/bin/qmail-qread command)
```

cPanel:

```
/var/log/exim_mainlog
```

```
/var/log/exim_paniclog
```

/var/log/exim\_rejectlog

/var/log/mailllog exim -bpr | grep "<" | wc -l (View the amount of messages currently in your outbound queue)

exim -bp (List out all messages in your outbound queue)

cPanel also has a graphical mail queue layout that you can view inside WebHost Manager by going to Email > Mail Queue Manager. Simple Control Panel:

/var/log/mailllog (Postfix Log)

mailq (List out all messages in your outbound queue)

postcat -q \$mailq\_message\_number | more (Read the contents of an email in your outbound queue)

Plesk Windows Servers:

All mail related messages are stored in text files on the server. To view messages in the outbound queue, browse to:

C:%Plesk Directory%\PleskMail ServersMail EnableQueuesSMTPOutgoing

C:%Plesk Directory%\PleskMail ServersMail EnableQueuesSMTPInbound (for incoming)

Right click on any of these files and open in Notepad. NOTE:Your mail logs may also detail

vulnerabilities in any scripts that you have installed that send mail. Injection attacks are common

against scripts that do not check header data. A trend that indicates an injection attack is a large

number of addresses in the BCC field of emails in your queue.[Check Exim Mail Settings in cPanel](#)On

cPanel servers, make sure you have :fail: instead of :blackhole: for your Exim mail settings. An article

at <http://www.configserver.com/free/fail.html> details the differences between the two settings.To set

the default mail behavior to :fail:, you will want to execute the following command through SSH:echo

"defaultmailaction=fail" >> /var/cpanel/cpanel.configIf your domains are set to :fail:, and your logs still

show suspicious traffic that leads to continuous relay usage, then you most likely have problems with

the Exim Callout system.By default, exim.conf is set to use callouts to verify the existence of email

senders. This means that every time an email is sent to your server from a new address, Exim

connects to the relay server during the RCPT callout command. This places an entry into the Exim

"mainlog" and uses a SMTP relay.You can disable this feature by following these steps:Log into

WebHost Manager Click on Exim Configuration Editor under the Service Configuration area of the

left-hand toolbar. In the second gray area titled Options you will see 4 checkboxes Uncheck the third

checkbox Use callouts to verify the existence of email senders Click Save