

Configuring SMTP Relay Server

If you have been affected by the recent block of outgoing mail on port 25 for our SoftLayer locations, you will be able to use the following to configure another server in Salt Lake City, New York, London, or Amsterdam to relay your email. Make sure that before you utilize this guide you purchase a new server, preferably SSD VPS via your account at <https://console.100tb.com>. Please follow the steps below to complete this task.

****Please keep in mind that support cannot assist with the configuration of your new SMTP relay server. You would be required to purchase Supreme Support in order to receive assist with any configuration changes.**

Step-by-Step Guide

We will first walk you through how to configure your current server to communicate with your new relay server on a port other than 25. Please follow the appropriate steps below based on the mail server you are currently using.

For Postfix:

1. Navigate to the following location:

```
#> vi /etc/postfix/main.cf
```

2. Insert the following line and save:

```
relayhost = <IP_address_of_new_server>:587
```

3. Restart Postfix:

```
#> postfix stop && postfix start  
#> /etc/init.d/postfix restart
```

For Exim:

1. Navigate to the Exim configuration file:

```
#> vi /etc/exim/exim.conf
```

2. Insert the following in the routers section (after begin routers) and save:

```
spamgateway_smarthost_router:  
  driver = manualroute  
  transport = spamgateway_smarthost_transport  
  route_list = * <IP_address_of_new_server>::587  
  no_more
```

3. Restart Exim:

```
#> service exim restart **or** /etc/init.d/exim restart
```

For cPanel/WHM:

1. Log into WHM and navigate to Mail -> Server Configuration -> Exim Configuration Manager
2. Inside the Basic Editor locate the Smarthost support option
3. Insert the <IP_address_of_new_server> in the text box and SAVE

Exim Configuration Manager

Basic Editor Advanced Editor Backup Restore Reset

Options in *italics* are unavailable because of other options that are set.

< All ACL Options Access Lists Domains and IPs Filters Mail RBLs Security Apache SpamAssassin™ Options > Find

Log sender rates in the exim mainlog. This can be helpful for tracking problems and/or spammers.	<input type="radio"/> On <input checked="" type="radio"/> Off <i>default</i>
Sender Verification Callouts [?]	<input type="radio"/> On <input checked="" type="radio"/> Off <i>default</i>
Smarthost support [?]	<input type="radio"/> <i>default</i> <input checked="" type="radio"/> <input type="text"/>
EXPERIMENTAL: Rewrite From: header to match actual sender [?]	<input type="radio"/> remote <input type="radio"/> all <input checked="" type="radio"/> <i>disable default</i>
Send generic recipient failure messages [?]	<input type="radio"/> On <input checked="" type="radio"/> Off <i>default</i>
Allow mail delivery if malware scanner fails [?]	<input checked="" type="radio"/> On <input type="radio"/> Off <i>default</i>
Bounce email for users over quota [?]	<input checked="" type="radio"/> On <input type="radio"/> Off <i>default</i>

All configurations have now been made to the current server and you can move to configuring the new server intended as the relay server. Please follow the steps below to configure your mail server on the new server.

Please ensure that this new server is installed with a RHEL/CentOS 6 distribution able to support Exim mail server and do the following:

Ensure we have the latest EPEL repository RPM for CentOS 6 64-bit on the new server and then follow the steps below.

```
#> wget http://download.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
#> rpm -ivh epel-release-6-8.noarch.rpm
```

1. Install Exim mail server via yum:

```
#> yum install -y exim-mysql
```

2. Stop the Postfix and enable Exim server:

```
#> service postfix stop
#> chkconfig postfix off
```

3. Set Exim as the default MTA:

```
#> alternatives --config mta
There are 2 programs which provide 'mta'.

Selection    Command
-----
*+ 1         /usr/sbin/sendmail.postfix
   2         /usr/sbin/sendmail.exim

Enter to keep the current selection[+], or type selection number: 2
```

4. Set auto start on boot and start the exim service:

```
#> chkconfig exim on
#> service exim start
```

5. Now that the Exim server is installed and running you must add the <IP_of_current_server> to the exim.conf file:

```
#> vi /etc/exim/exim.conf
```

6. Inside exim.conf locate "hostlist relay_from_hosts =" and add the IP of your current server and save the file:

```
hostlist relay_from_hosts = <IP_address_of_current_server>
```

****Please check how many IPs are assigned to the current server. Exim can send emails from more than one IP. All these IPs should be added to the Exim configuration on Relay side. The IPs must be separated by ":"**

```
hostlist relay_from_hosts = 127.0.0.1 : <additional_ip> : <additional_ip> : <additional_ip>
```

7. Restart Exim

```
#> service exim restart
#> /etc/init.d/exim restart
```

You have now configured all mail on your server affected by the block of port 25 to utilize your recently configured SMTP relay server. Please test this by sending from your current server affected by the block and see if the mail is received.

In order to avoid your messages being marked as SPAM please make sure you do the following:

1. New relay server MUST have a valid hostname. You must use a fully-qualified domain name (FQDN) that contains two periods (for example: [host name.example.com](#)).
2. rDNS must be set on the new relay server IP
3. Add the New_Relay_Server_IP to the SPF record for every domain. Please reference the example below:

```
example.com      IN TXT      "v=spf1 a:<current_server_IP>mx:<new_relay_server_IP> ~all"
```

If you have any questions, please feel free to contact us via a ticket through your Console account and we will be able to assist you.