



Sendmail Configuration Guide

Mail Prove RBL Service

Version: 1.3

Prepared by:

Mail Proved Limited

July 30, 2004

Mail Prove Limited

Unit 806, Cyberport 1
100 Cyberport Road
Pokfulam, Hong Kong

郵盾亞洲有限公司

香港灣仔
數碼港道100號
數碼港1座806室

Tel 電話 (852) 3105 2920

Fax 傳真 (852) 3105 2926

Email 電郵 info@MailProve.com

www.MailProve.com

Revision History

Date	Version	Description	Made by
Jul 30, 2004	1.3	How to add X-RBL-Warning header to email	Henry Cheng
Feb 21, 2004	1.2	Revised service options	Seve Ho
Feb 13, 2004	1.1	Configuration options added	Seve Ho
Jan 04, 2004	1.0	First version of document	Seve Ho

Introduction

This configuration guide provides guidelines to configure different MTA to use Mail Prove Service.

Sendmail Configuration Guide

Enabling Mail Prove RBL Service in Sendmail can be achieved by one of the two methods:

- Method A: Edit Sendmail configuration marco file and regenerate new configuration file.
- Method B: Edit Sendmail configuration file directly.
- Method C (Special): Edit Sendmail configuration macro and Sendmail configuration file such that any email come from blacklisted MTA are added with a X-RBL-Warning header instead of being rejected.

Cautions: Method A is suggested as Method B is prone to errors and may lead to unexpected behaviors of Sendmail.

Method A: Edit Sendmail configuration marco file and regenerate new configuration file.

1. Login to the system with root privilege.

2. Backup old Sendmail Configuration File

```
# cp /<sendmail source>/sendmail.cf /<sendmail source>/sendmail.cf.bk
```

where <sendmail source> is the directory where Sendmail is installed.

3. Edit the Sendmail configuration marco file.

```
# vi <sendmail source>/sendmail.mc
```

4. Add "Use RBL Feature" options to marco file by typing following lines,

```
FEATURE(dnsbl, `c10.rbl.hk', ``550 Rejected: This system is protected by Mail Prove Service, " ${client_addr} " is blacklisted, please go to www.mailprove.com to unblock."')
```

You should replace "c10.rbl.hk" with the RBL Domain provided by MailProve.

The second argument is the error message to be attached to the bounce mail sent back to the spam sender. Default error message is used if empty string is used which is,

```
Rejected: IP-ADDRESS listed at SERVER
```

where “IP-ADDRESS” and “SERVER” are replaced by the appropriate information.

6. Generate New Sendmail Configuration File

```
# m4 sendmail.mc > sendmail.cf
```

7. Restart Sendmail

Method B: Edit Sendmail configuration file directly

1. Login to the system with root privilege.

2. Backup Sendmail configuration file.

```
# cp sendmail.cf sendmail.cf.bk
```

3. Edit the Sendmail configuration file.

```
# vi <sendmail source>/sendmail.cf
```

where <sendmail source> is the directory where Sendmail is installed.

4. The configuration file consists several parts, starting of each part is surrounded by '*' sign, eg.

```
#####  
# Local info #  
#####
```

5. Find "Local info" part and add options "map for DNS based blacklist lookups" before the last options of "Local info", i.e "Configuration version number". It will look like following,

```
#####  
# local info #  
#####  
  
# map for DNS based blacklist lookups  
Kdnsbl host -T<TMP>  
  
# Configuration version number  
DZ8.12.9  
  
#####  
# Options #  
#####
```

Remark: For Sendmail compiled with IPv6 support, set 'Kdnsbl' as following instead,

```
# map for DNS based blacklist lookups  
Kdnsbl dns -R A -T<TMP>
```

6. Depends on your preference, in occurrence of “Temporary Lookup Failure”(The RBL is not responding on certain lookup request), you may want to:

- (a) reject the email or
- (b) accept mail.

(a) Find “check_relay -- check hostname/address on SMTP startup”, and add the following text,

```
# DNS based IP address spam list c10.rbl.hk
R$*<TABx3>$: $&{client_addr}
R$-.$-.$-.$<TABx2>$: <?> $(dnsbl $4.$3.$2.$1.c10.rbl.hk. $: OK $)
R<?>OK<TABx3>$: OKSOFAR
R<?>${+<TMP><TABx2>$#error $@ 4.7.1 $: "451 Temporary lookup failure of " $&
{client_addr} " "
R<?>${+<TABx3>$#error $@ 5.7.1 $: "550 Rejected: This system is protected by Mail
Prove Service, " $&{client_addr} " is blacklisted, please go to www.mailprove.com to
unblock."
```

where c10.rbl.hk should be replaced with RBL Domain provided by MailProve.

Remark: <TABx3> and <TABx2> represents 3 and 2 tabs in between texts and “NO SPACE” is needed.

The text should look like the following:

```
# DNS based IP address spam list c10.rbl.hk
R$*
R$-.$-.$-.$
R<?>OK
R<?>${+<TMP>
R<?>${+
$: ${client_addr}
$: <?> $(dnsbl $4.$3.$2.$1.c10.rbl.hk. $: OK $)
$: OKSOFAR
$: "451 IP: " ${client_addr} " lookup failed."
$: "550 Rejected: This system is protected by Mail Prove Service, " ${client_addr} $
```

(b) To ignore “Temporary Lookup Failure”(accept email when RBL service is unreachable temporary), find “check_relay -- check hostname/address on SMTP startup”, and add the following text,

```
# DNS based IP address spam list c10.rbl.hk
R$*<TABx3>$: $&{client_addr}
R$-.$-.$-.$<TABx2>$: <?> $(dnsbl $4.$3.$2.$1.c10.rbl.hk. $: OK $)
R<?>OK<TABx3>$: OKSOFAR
R<?>${+<TMP><TABx2>$: TMPOK
R<?>${+<TABx3>$#error $@ 5.7.1 $: "550 Rejected: This system is protected by Mail
Prove Service, " $&{client_addr} " is blacklisted, please go to www.mailprove.com to
unblock."
```

where c10.rbl.hk should be replaced with RBL Domain provided by MailProve.

Remark: <TABx3> and <TABx2> represents 3 and 2 tabs in between texts and “NO SPACE” is needed.

The text should look like the following:

```
# DNS based IP address spam list c10.rbl.hk
R$*                               $: ${client_addr}
R$-.$-.$-.$-                     $: <?> $(dnsbl $4.$3.$2.$1.c10.rbl.hk. $: OK $)
R<?>OK                             $: OKSOFAR
R<?>.$+<TMP>                       $: TMPOK
R<?>.$+                             $#error %0 5.7.1 $: "550 Rejected: This system is protected by Mail Prove Service, " ${client_addr} $
```

7. Restart Sendmail

Method C (Special): Edit Sendmail configuration macro and Sendmail configuration file such that any email come from blacklisted MTA are added with a X-RBL-Warning header instead of being rejected.

1. Login to the system with root privilege.

2. Backup old Sendmail Configuration File

```
# cp /<sendmail source>/sendmail.cf /<sendmail source>/sendmail.cf.bk
```

where <sendmail source> is the directory where Sendmail is installed.

3. If your Sendmail configuration file (sendmail.cf) is generated from Sendmail configuration macro file (sendmail.mc), please goto step (4) – (6) and skip step (7) – (10). Otherwise skip step (4) – (6) and goto step (7) – (10).

4. Edit the Sendmail configuration marco file.

```
# vi <sendmail source>/sendmail.mc
```

5. Add “Use RBL Feature” options to marco file by typing following lines,

```
FEATURE(dnsbl, `c10.rbl.hk', `''')
```

You should replace “c10.rbl.hk” with the RBL Domain provided by MailProve.

6. Generate New Sendmail Configuration File

```
# m4 sendmail.mc > sendmail.cf
```

7. If your Sendmail configuration file (sendmail.cf) is **NOT** generated from Sendmail configuration macro file (sendmail.mc), edit the Sendmail configuration file.

```
# vi <sendmail source>/sendmail.cf
```

where <sendmail source> is the directory where Sendmail is installed.

8. The configuration file consists several parts, starting of each part is surrounded by '*' sign, eg.

```
#####  
# Local info #  
#####
```

9. Find "Local info" part and add options "map for DNS based blacklist lookups" before the last options of "Local info", i.e "Configuration version number". It will look like following,

```
#####  
# local info #  
#####  
  
# map for DNS based blacklist lookups  
Kdnsbl host -T<TMP>  
  
# Configuration version number  
DZ8.12.9  
  
#####  
# Options #  
#####
```

Remark: For Sendmail complied with IPv6 support, set 'Kdnsbl' as following instead,

```
# map for DNS based blacklist lookups  
  
Kdnsbl dns -R A -T<TMP>
```

10. Depends on your preference, in occurrence of “Temporary Lookup Failure”(The RBL is not responding on certain lookup request), you may want to:

- (a) **reject the email** or
- (b) **accept mail.**

(a) Find “check_relay -- check hostname/address on SMTP startup”, and add the following text,

```
# DNS based IP address spam list c10.rbl.hk
R$*<TABx3>$: $&{client_addr}
R$-.$-.$-.$<TABx2>$: <?> $(dnsbl $4.$3.$2.$1.c10.rbl.hk. $: OK $)
R<?>OK<TABx3>$: OKSOFAR
R<?>${+<TMP><TABx2>}$#error $@ 4.7.1 $: "451 Temporary lookup failure of " $&
{client_addr} " "
R<?>${+<TABx3>}$#error $@ 5.7.1 $: ""
```

where c10.rbl.hk should be replaced with RBL Domain provided by MailProve.

Remark: <TABx3> and <TABx2> represents 3 and 2 tabs in between texts and “NO SPACE” is needed.

(b) To ignore “Temporary Lookup Failure”(accept email when RBL service is unreachable temporary), find “check_relay -- check hostname/address on SMTP startup”, and add the following text,

```
# DNS based IP address spam list c10.rbl.hk
R$*<TABx3>$: $&{client_addr}
R$-.$-.$-.$<TABx2>$: <?> $(dnsbl $4.$3.$2.$1.c10.rbl.hk. $: OK $)
R<?>OK<TABx3>$: OKSOFAR
R<?>${+<TMP><TABx2>}$: TMPOK
R<?>${+<TABx3>}$#error $@ 5.7.1 $: ""
```

where c10.rbl.hk should be replaced with RBL Domain provided by MailProve.

Remark: <TABx3> and <TABx2> represents 3 and 2 tabs in between texts and “NO SPACE” is needed.

11. Open sendmail.cf and update it as the following.

(a) Find the following lines in sendmail.cf

```
# arithmetic map
Karith arith
```

then append the following lines if they are not found in original sendmail.cf

```
# macro storage map
Kmacro macro

# Declare Macro – DNSbl_Header (must be included if Sendmail version < 8.12)
D{DNSbl_Header}

# The macro we will use to store the warning
C{persistentMacros}{DNSbl_Header}

# Header to Add
H?${DNSbl_Header}?X-RBL-Warning: ${client_addr} is blacklisted.
```

Remark: You can update the text after X-RBL-Warning as your preference.

(b) Find the following lines in sendmail.cf

```
R<?>${<TABx3>}#error $@ 5.7.1 $: ""
```

then update it as the following lines

```
R<?>${<TABx3>}$: $( macro {DNSbl_Header} $@ $1 $)
```

Remark: <TABx3> represents 3 tabs in between texts and “NO SPACE” is needed.

12. Restart Sendmail