

Internet Draft
Document: [draft-elvey-refuse-sieve](#)
Expires: December 2004

M. Elvey
The Elvey Partnership, LLC
A. Melnikov
Isode Ltd
June 2004

The SIEVE mail filtering language - refuse extension
draft-elvey-refuse-sieve-02.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

This memo defines the SIEVE mail filtering language [[SIEVE](#)] "refuse" extension.

A Joe-job is a spam run forged to appear as though it came from an innocent party, who is then generally flooded by the bounces, MDNs and messages with complaints. With the Sieve "reject" action, MDNs contribute to the flood of Joe-job spam to victims of Joe-jobs; SMTP level refusals usually don't. With "refuse", Sieve gains the ability to simply not accept an email during the SMTP transaction (instead of accepting it and then sending an MDN [[MDN](#)] back to the alleged sender using "reject").

Table of Contents

1. Discussion	2
2. Conventions Used in this Document	3
3. Introduction and Overview	3

4. SIEVE Extension	4
4.1 Action refuse	4
4.2 "refuse" compatibility with other actions	5
4.3 Explicit accomodation for servers that support Enhanced Error Codes [ENHANCED-CODES]	5
5. Security Considerations	5
6. IANA Considerations	6
6.1 refuse extension registration	6
7. References	6
7.1 Normative References	6
7.2 Informative References	7
8. Acknowledgments	7
9. Author's Addresses	7
10. Intellectual Property Rights Statement	7
11. Full Copyright Statement	8
12. Change Log	8

1. Discussion

The SIEVE mail filtering language [[SIEVE](#)] "refuse" extension, if supported, permits users to handle unwanted email in a way that is sometimes preferable to the existing 'discard' and 'reject' capabilities. When a spam-detection system suspects a message is spam, but isn't certain, discarding the email is considered too risky for some users, for example, those who receive sales leads by email. They are willing to use the reject command. Users are willing to reject but not discard because the sender of an email incorrectly marked as spam will receive a notification that the email was refused, and will likely try again to contact the intended recipient, perhaps via another method of communication. Unfortunately, this usage is problematic, because in the usual case, the email is indeed spam, and the alleged sender to whom the MDN caused by the reject will be sent will often be an innocent Joe-job victim. "Refuse" is intended to be superior to "reject" because it will be less likely to result in email to an innocent victim. "Refuse" refuses to accept an email for delivery instead of accepting it and then sending an MDN. Much spam is sent through open proxies, so "refuse" reduces Joe-job bounces resulting from usage of reject. "Refuse" will also reduce Joe-jobs caused by virus self-propagation via emails with false sender information. "Refuse" may conserve bandwidth, by reducing the number of MDNs sent. Further discussion highlighting the risks of "reject" and the benefits of "refuse" can be found in [[Joe-DoS](#)].

2. Conventions Used in this Document

Conventions for notations are as in [[SIEVE](#)] [section 1.1](#), including use of [[KEYWORDS](#)].

This document does not attempt to define what exactly constitutes a

spam or virus containing email or how it should be identified, or what actions should be taken when detected.

[3.](#) Introduction and Overview

The "refuse" action MUST refuse to accept an email for delivery at the SMTP/LMTP level by returning a 5XX reply code, instead of sending an MDN as required by the "reject" action, other than for the two exceptions specified below. A SIEVE implementation that cannot do so MUST NOT claim to support the refuse extension.

There is an exception when a message has multiple valid recipients, and at least one but not all of them are refusing delivery (whether the refusal is caused by execution of a Sieve "refuse" or for another reason). In this case, the server MUST accept the message and generate DSNs for all recipients that are refusing it. Note that this exception only applies to SMTP, as LMTP is able to reject messages on a per-recipient basis.

If a "refuse" implementation performs a return-path verification and it clearly indicates that the message has a forged return-path, the implementation need not refuse to accept the mail, but rather MAY accept and discard it.

[4.](#) SIEVE Extension

This section defines the "refuse" action.

[4.1](#) Action refuse

Syntax: `refuse <reason: string>`

The "refuse" action refuses delivery of a message by sending back the 550 SMTP response code to an SMTP client.

This extension can be only supported by a Sieve implementation running in a MTA.

Note that SMTP [[SMTP](#)] doesn't allow for non-ASCII characters in SMTP response text. It is an error for non-ASCII characters to appear in the "reason" string (unless the client and the server use an SMTP extension that allows for transmission of non-ASCII reply text; such an extension is not known to the authors).

If the "reason" string is multiline, than the reason text MUST be returned as a multiline SMTP/LMTP response, per [[SMTP](#)], [section 4.2.1](#).

In the following script (which assumes support for the spamtest

extension), messages that test highly positive for spam are refused.

Example:

```
require ["refuse", "spamtest"]
```

```
if spamtest :value "ge" :comparator "i;ascii-numeric" "6" {  
    refuse text:
```

SpamAssassin thinks the message is spam.

It is therefore being refused.

Please call 1-900-PAY-US if you want to reach us.

.

```
    ;  
    elsif spamtest :value "ge" :comparator "i;ascii-numeric" "4" {  
        fileinto "Suspect";  
    }
```

The following excerpt from an SMTP session shows it in action.

.

C: DATA

S: 354 Send message, ending in CRLF.CRLF.

...

C: .

S: 550-SpamAssassin thinks the message is spam.

S: 550-It is therefore being refused.

S: 550 Please call 1-900-PAY-US if you want to reach us.

SIEVE implementations that implement the "refuse" action must use the "refuse" capability string.

[4.2](#) "refuse" compatibility with other actions

"Refuse" cancels the implicit keep, and is incompatible with "reject" and "discard". "Refuse" is also incompatible with "vacation" extension [VACATION]. (It should be compatible and incompatible with the same actions as "reject", but [SIEVE] states "Implementations SHOULD prohibit reject when used with other actions." However we feel that "refuse" should be permitted when used with other actions such as "fileinto" and "redirect". This could be useful for analyzing, tracking or reporting spam. Also, users can use tricks (such as multiple redirects back to their own email addresses) to get around such a prohibition anyway.)

[4.3](#) Explicit accomodation for servers that support Enhanced Error Codes [ENHANCED-CODES]

This section only concerns implementations that support Enhanced Error Codes.

If the server supports [RFC 2034](#) [[ENHANCED-CODES](#)] it MUST select an appropriate Enhanced Error Code (e.g. 5.7.1 or a more generic 5.7.0) and prepend it to the "reason" text. I.e. on such an implementation, the example in [section 4.1](#) would show up in SMTP as:

```
550-5.7.1 SpamAssassin thinks the message is spam.  
550-5.7.1 It is therefore being refused.  
550 5.7.1 Please call 1-900-PAY-US if you want to reach us.
```

if the server selected "5.7.1" as appropriate.

[5.](#) Security Considerations

The "refuse" extension does not raise any security considerations that are not present in the base [[SIEVE](#)] protocol, and these issues are discussed in [[SIEVE](#)].

[6.](#) IANA Considerations

The following section provides the IANA registration for the Sieve extensions specified in this document:

[6.1](#) refuse extension registration

To: iana@iana.org
Subject: Registration of new Sieve extension

Capability name: refuse
Capability keyword: refuse
Capability arguments: N/A
Standards Track/IESG-approved experimental RFC number: this RFC
Person and email address to contact for further information:

Matthew Elvey
The Elvey Partnership, LLC
3042 Sacramento-ietf St Ste 04
San Francisco, CA
U.S.A.

<<mailto:sieve3@matthew.elvey.com>>

[7.](#) References

[7.1](#) Normative References

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", [RFC 2119](#), March 1997.

[SIEVE] Showalter, "Sieve: A Mail Filtering Language", [RFC 3028](#), January 2001.

[SMTP] Klensin, J. (Editor), "Simple Mail Transfer Protocol", AT&T Laboratories, [RFC 2821](#), April 2001.

[LMTP] Myers, J., "Local Mail Transfer Protocol", Carnegie-Mellon University, [RFC 2033](#), October 1996.

[DSN] Moore, K., Vaudreuil, G., "An Extensible Message Format for Delivery Status Notifications", University of Tennessee, Lucent Technologies, [RFC 3464](#), January 2003.

[MDN] Fajman, R., "An Extensible Message Format for Message Disposition Notifications", National Institutes of Health, [RFC 2298](#), March 1998.

[ENHANCED-CODES] Freed, N., "SMTP Service Extension for Returning Enhanced Error Codes", Innosoft, [RFC 2034](#), October 1996.

[7.2](#) Informative References

[Joe-DoS] Stefan Frei, Ivo Silvestri, Gunter Ollmann, "Mail Non Delivery Message DDoS Attacks", 5 April 2004;
<http://www.techzoom.net/paper-mailbomb.asp>

[8.](#) Acknowledgments

Thanks to Ned Freed, Cyrus Daboo, Arnt Gulbrandsen and Mark E. Mallett for comments and corrections.

[9.](#) Author's Addresses

Matthew Elvey
The Elvey Partnership, LLC
3042 Sacramento-ietf St Ste 04
San Francisco, CA
U.S.A.

Email: sieve3@matthew.elvey.com

Alexey Melnikov
Isode Limited
5 Castle Business Village
36 Station Road

Hampton, Middlesex, TW12 2BX
UK

Email: Alexey.Melnikov@isode.com

10. Intellectual Property Rights Statement

This document is an Internet-Draft and is subject to all provisions of [Section 10 of RFC2026](#).

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

11. Full Copyright Statement

Copyright (C) The Internet Society 2004. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF

THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

12. Change Log

- 00 First formal draft.
- 01 Explicit [RFC 2034](#) support, disallow "refuse" in MUAs, typos corrected, clarifications, etc.
- 02 Many insubstantial editorial changes (mostly rewording text for readability). Added text regarding non-ASCII characters in the refuse "reason" string. Added an exception allowing return-path forgery to justify discarding a message.