

The SYS and AUTH POP Response Codes

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

This memo proposes two response codes: SYS and AUTH, which enable clients to unambiguously determine an optimal response to an authentication failure. In addition, a new capability (AUTH-RESP-CODE) is defined.

Table of Contents

1. Introduction	2
2. Conventions Used in this Document	2
3. Background	2
4. The SYS Response Code	3
5. The AUTH Response Code	3
6. The AUTH-RESP-CODE Capability	4
7. IANA Considerations	4
8. Security Considerations	4
9. References	5
10. Author's Address	5
11. Full Copyright Statement	6

1. Introduction

RFC 2449 [POP3-EXT] defined extended [POP3] response codes, to give clients more information about errors so clients can respond more appropriately. In addition to the mechanism, two initial response codes were defined (IN-USE and LOGIN-DELAY), in an attempt to differentiate between authentication failures related to user credentials, and other errors.

In practice, these two response codes, while helpful, do not go far enough. This memo proposes two additional response codes: SYS and AUTH, which enable clients to unambiguously determine an optimal response to an authentication failure.

In addition, a new capability (AUTH-RESP-CODE) is defined.

2. Conventions Used in this Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [KEYWORDS].

3. Background

RFC 2449 [POP3-EXT] introduced the IN-USE and LOGIN-DELAY response codes. The intent is to allow clients to clearly determine the underlying cause of a failure in order to respond. For example, clients need to know if the user should be asked for new credentials, or if the POP3 session should simply be tried again later. (Some deployed POP3 clients attempt to parse the text of authentication failure errors, looking for strings known to be issued by various servers which indicate the mailbox is locked.)

IN-USE indicates that an exclusive lock could not be obtained for the user's mailbox, probably because another POP3 session is in progress. LOGIN-DELAY informs the client that the user has not waited long enough before authenticating again.

However, there are other error conditions which do not require new credentials, some of which should be brought to the user's attention.

Despite the IN-USE and LOGIN-DELAY responses, clients cannot be sure if any other error requires new user credentials.

4. The SYS Response Code

The SYS response code announces that a failure is due to a system error, as opposed to the user's credentials or an external condition. It is hierarchical, with two possible second-level codes: TEMP and PERM. (Case is not significant at any level of the hierarchy.)

SYS/TEMP indicates a problem which is likely to be temporary in nature, and therefore there is no need to alarm the user, unless the failure persists. Examples might include a central resource which is currently locked or otherwise temporarily unavailable, insufficient free disk or memory, etc.

SYS/PERM is used for problems which are unlikely to be resolved without intervention. It is appropriate to alert the user and suggest that the organization's support or assistance personnel be contacted. Examples include corrupted mailboxes, system configuration errors, etc.

The SYS response code is valid with an -ERR response to any command.

5. The AUTH Response Code

The AUTH response code informs the client that there is a problem with the user's credentials. This might be an incorrect password, an unknown user name, an expired account, an attempt to authenticate in violation of policy (such as from an invalid location or during an unauthorized time), or some other problem.

The AUTH response code is valid with an -ERR response to any authentication command including AUTH, USER (see note), PASS, or APOP.

Servers which include the AUTH response code with any authentication failure SHOULD support the CAPA command [POP3-EXT] and SHOULD include the AUTH-RESP-CODE capability in the CAPA response. AUTH-RESP-CODE assures the client that only errors with the AUTH code are caused by credential problems.

NOTE: Returning the AUTH response code to the USER command reveals to the client that the specified user exists. It is strongly RECOMMENDED that the server not issue this response code to the USER command.

6. The AUTH-RESP-CODE Capability

CAPA tag:

AUTH-RESP-CODE

Arguments:

none

Added commands:

none

Standard commands affected:

none

Announced states / possible differences:

both / no

Commands valid in states:

n/a

Specification reference:

this document

Discussion:

The AUTH-RESP-CODE capability indicates that the server includes the AUTH response code with any authentication error caused by a problem with the user's credentials.

7. IANA Considerations

IANA has added the AUTH-RESP-CODE capability to the list of POP3 capabilities (established by RFC 2449 [POP3-EXT]).

IANA has also added the SYS and AUTH response codes to the list of POP3 response codes (also established by RFC 2449 [POP3-EXT]).

8. Security Considerations

Section 5, The AUTH Response Code, discusses the security issues related to use of the AUTH response code with the USER command.

9. References

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[POP3] Myers, J. and M. Rose, "Post Office Protocol -- Version 3", STD 53, RFC 1939, May 1996.

[POP3-EXT] Gellens, R., Newman, C. and L. Lundblade, "POP3 Extension Mechanism", RFC 2449, November 1998.

10. Author's Address

Randall Gellens
QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121-2779
U.S.A.

Phone: +1 858 651 5115
EMail: randy@qualcomm.com

11. Full Copyright Statement

Copyright (C) The Internet Society (2002). 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.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

