

[MS-STANXPOP3]: Exchange Post Office Protocol Version 3 (POP3) Standards Compliance

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: <http://www.microsoft.com/interop/osp>) or the Community Promise (available here: <http://www.microsoft.com/interop/cp/default.mspx>). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplq@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
07/15/2009	1.0.0	Major	Initial Availability.
10/01/2008	1.1.0	Minor	Updated IP notice.
04/10/2009	2.0.0	Major	Updated applicable product releases.
07/15/2009	3.0.0	Major	Revised and edited technical content.
11/04/2009	4.0.0	Major	Updated and revised the technical content.
02/10/2010	4.0.0	None	Version 4.0.0 release

Table of Contents

1 Introduction	4
1.1 Glossary	4
1.2 Normative References	4
1.3 Informative References	5
1.4 Microsoft Implementations	5
1.5 Conformance Requirements	5
1.6 Notation	6
2 Conformance Statements	7
2.1 Normative Variations	7
2.1.1 [RFC1939] Section 3, Separation by SPACE Character	7
2.1.2 [RFC1939] Section 3, Argument Length	7
2.1.3 [RFC1939] Section 4, Exclusive-Access Lock on Maildrop	7
2.1.4 [RFC1939] Section 5, Maildrop Size Returned by STAT Command	7
2.1.5 [RFC1939] Section 5, Message Size Returned by LIST Command	7
2.2 Clarifications	8
2.2.1 [RFC1939] Section 3, Basic Operation	8
2.2.2 [RFC1939] Section 4, The AUTHORIZATION State	9
2.2.3 [RFC1939] Section 5, STAT Command	10
2.2.4 [RFC1939] Section 5, LIST Command	10
2.2.5 [RFC1939] Section 6, QUIT Command	10
2.2.6 [RFC1939] Section 7, TOP Command	10
2.2.7 [RFC1939] Section 7, UIDL Command	11
2.2.8 [RFC1939] Section 7, USER Command	11
2.2.9 [RFC1939] Section 7, PASS Command	12
2.2.10 [RFC1939] Section 7, APOP Command	12
2.2.11 [RFC1939] Section 8, Scaling and Operational Considerations	13
2.2.12 [RFC1939] Section 11, Message Format	13
2.2.13 [RFC2449] Section 4, Maximum Length of Command	13
2.2.14 [RFC2449] Section 4, Commands Up To 255 Octets	14
2.3 Error Handling	14
2.4 Security	14
3 Change Tracking	15
4 Index	16

1 Introduction

This document specifies the level of support provided by the **Post Office Protocol - Version 3 (POP3)** service for Microsoft Exchange Server 2007 and Microsoft Exchange Server 2010. The POP3 service for Exchange Server is used by clients that implement the POP3 protocol to store and retrieve **messages** on the server.

1.1 Glossary

The following terms are defined in [\[MS-OXGLOS\]](#):

message
Carriage Return Line Feed (CRLF)
Generic Security Service Application Program Interface (GSSAPI)
Post Office Protocol - Version 3 (POP3)
Secure Sockets Layer (SSL)
Transmission Control Protocol (TCP)
Transport Layer Security (TLS)

The following terms are specific to this document:

CAS: Client Access Server

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [\[RFC2119\]](#). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, <http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624>, as an additional source.

[MS-NLMP] Microsoft Corporation, "NT LAN Manager (NTLM) Authentication Protocol Specification", July 2006, <http://go.microsoft.com/fwlink/?LinkId=111472>.

[MS-OXGLOS] Microsoft Corporation, "[Exchange Server Protocols Master Glossary](#)", June 2008.

[MS-OXPOP3] Microsoft Corporation, "[Post Office Protocol Version 3 \(POP3\) Extensions](#)", June 2008.

[RFC822] Crocker, D.H., "STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES", RFC 822, August 1982, <http://www.ietf.org/rfc/rfc0822.txt>.

[RFC1939] Myers, J. and Rose, M., "Post Office Protocol - Version 3", RFC 1939, May 1996, <http://www.ietf.org/rfc/rfc1939.txt>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>.

[RFC2246] Dierks, T. and Allen, C., "The TLS Protocol Version 1.0", RFC 2246, January 1999, <http://www.ietf.org/rfc/rfc2246.txt>.

[RFC2449] Gellens, R., Newman, C., and Lundblade, L., "POP3 Extension Mechanism", RFC 2449, November 1998, <http://www.ietf.org/rfc/rfc2449.txt>.

[RFC3546] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and Wright, T., "Transport Layer Security (TLS) Extensions", RFC 3546, June 2003, <http://www.ietf.org/rfc/rfc3546.txt>.

[RFC4121] Zhu, L., Jaganathan, K., and Hartman, S., "The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2", RFC 4121, July 2005, <http://www.ietf.org/rfc/rfc4121.txt>.

[RFC4616] K. Zeilenga and the OpenLDAP Foundation, "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism", RFC 4616, August 2006, <http://www.ietf.org/rfc/rfc4616.txt>.

1.3 Informative References

[MSFT-SETIMAP] Microsoft Corporation, "Set-IMAPSettings", <http://go.microsoft.com/fwlink/?LinkId=154303>.

1.4 Microsoft Implementations

Microsoft Exchange Server 2007

Microsoft Exchange Server 2010

1.5 Conformance Requirements

The conformance requirements for [\[RFC1939\]](#) and [\[RFC2449\]](#) are that all required portions of the specifications are implemented according to the specification, and any optional portions that are implemented are implemented according to the specification.

The following table lists the sections of [\[RFC1939\]](#) that are considered normative and the sections that are considered informative.

Section(s)	Normative/Informative
1 - 2	Informative
3 - 7	Normative
8 - 11	Informative
12	Normative
13 - 15	Informative

The following table lists the sections of [\[RFC2449\]](#) that are considered normative and the sections that are considered informative.

Section(s)	Normative/Informative
1	Informative
2 - 9	Normative
10 - 11	Informative
12	Normative
13 - 14	Informative

1.6 Notation

The following notations are used in this specification.

Notation	Explanation
C####	This identifies a clarification of ambiguity in the target specification. This includes imprecise statements, omitted information, discrepancies, and errata. This does not include data formatting clarifications.
V####	This identifies an intended point of variability in the target specification such as the use of MAY, SHOULD, or RECOMMENDED. This does not include extensibility points.
E####	Because the use of extensibility points (such as optional implementation-specific data) may impair interoperability, this profile identifies such points in the target specification.

2 Conformance Statements

2.1 Normative Variations

The following sub-sections detail the normative variations from [\[RFC1939\]](#).

2.1.1 [RFC1939] Section 3, Separation by SPACE Character

The specification states: "Keywords and arguments are each separated by a single SPACE character".

Exchange Server separates keywords and arguments by one or more SPACE characters, or one or more TAB characters.

2.1.2 [RFC1939] Section 3, Argument Length

The specification states: "Each argument may be up to 40 characters long."

Exchange Server does not validate the length of each argument. Instead, a default maximum command length of 512 octets is enforced. The maximum command length of any value can be modified by using the Exchange Management tools.

2.1.3 [RFC1939] Section 4, Exclusive-Access Lock on Maildrop

The specification states: "The POP3 server then acquires an exclusive-access lock on the maildrop, as necessary to prevent messages from being modified or removed before the session enters the UPDATE state. If the lock is successfully acquired, the POP3 server responds with a positive status indicator."

Exchange Server does not acquire an exclusive-access lock on the maildrop once a user successfully logs on.

2.1.4 [RFC1939] Section 5, Maildrop Size Returned by STAT Command

The specification states: "The positive response consists of "+OK" followed by a single space, the number of messages in the maildrop, a single space, and the size of the maildrop in octets."

By default, Exchange Server does not calculate the exact size of the maildrop in octets. Instead, the size is calculated based on the amount of storage the message actually occupies in storage. Exchange Server exposes a custom server setting, *EnableExactRFC822Size*, to enable size calculation based on the exact MIME size. For more information about the *EnableExactRFC822Size* parameter, see [\[MSFT-SETIMAP\]](#).

2.1.5 [RFC1939] Section 5, Message Size Returned by LIST Command

The specification states: "All POP3 servers are required to use a certain format for scan listings. A scan listing consists of the message-number of the message, followed by a single space and the exact size of the message in octets."

By default, Exchange Server does not calculate the exact size of the message in octets. Instead, the size is calculated based on the amount of storage the message actually occupies in storage. Exchange Server exposes a custom server setting, *EnableExactRFC822Size*, to enable size calculation based on the exact MIME size. For more information about the *EnableExactRFC822Size* parameter, see [\[MSFT-SETIMAP\]](#).

2.2 Clarifications

The following sub-sections identify clarifications relative to [\[RFC1939\]](#) and [\[RFC2449\]](#).

Additional Exchange POP3 extensions to [\[RFC1939\]](#) are as specified in [\[MS-OXPOP3\]](#).

2.2.1 [RFC1939] Section 3, Basic Operation

E0001:

The specification states: "Initially, the server host starts the POP3 service by listening on **TCP** port 110. When a client host wishes to make use of the service, it establishes a TCP connection with the server host."

Exchange 2007, Exchange 2010

By default, the Exchange POP3 server listens on TCP Port 110 (995 for **SSL**). However, the port bindings can be configured to any port by using the Exchange Management tools.

C0001:

The specification states: "Responses may be up to 512 characters long, including the terminating **CRLF**."

Exchange 2007, Exchange 2010

Exchange Server responses are a maximum of 512 characters long, including the terminating CRLF.

C0002:

The specification states: "Once the TCP connection has been opened and the POP3 server has sent the greeting, the session enters the AUTHORIZATION state. In this state, the client must identify itself to the POP3 server."

Exchange 2007, Exchange 2010

The client **MUST** identify itself to the server after it has received the greeting.

V0001:

The specification states: "There is no general method for a client to distinguish between a server which does not implement an optional command and a server which is unwilling or unable to process the command."

Exchange 2007, Exchange 2010

Exchange Server includes informational text after some negative responses to assist the client in determining the cause of the negative response.

V0002:

The specification states: "A POP3 server **MAY** have an inactivity autologout timer. Such a timer **MUST** be of at least 10 minutes' duration. The receipt of any command from the client during that interval should suffice to reset the autologout timer."

Exchange 2007, Exchange 2010

Exchange Server implements two inactivity timers. The authenticated timeout, which applies to sessions that are successfully authenticated, is set to 1,800 seconds by default. The unauthenticated timeout, which applies to unauthenticated sessions, is set to 60 seconds by default. The receipt of any command is sufficient to reset the inactivity timer. Both of these timeout values can be modified by using the Exchange Management tools.

V0003:

The specification states: "When the timer expires, the session does NOT enter the UPDATE state -- the server should close the TCP connection without removing any messages or sending any response to the client."

Exchange 2007, Exchange 2010

In the event of inactivity autologout, Exchange Server sends a response that notifies the client that the connection is being closed, prior to closing the connection.

2.2.2 [RFC1939] Section 4, The AUTHORIZATION State

C0003:

The specification states: "The client must now identify and authenticate itself to the POP3 server."

Exchange 2007, Exchange 2010

The client MUST now identify and authenticate itself to Exchange Server.

E0002:

The specification states: "While there is no single authentication mechanism that is required of all POP3 servers, a POP3 server must of course support at least one authentication mechanism."

Exchange 2007, Exchange 2010

Exchange Server supports the following authentication mechanisms:

- NTLM, as specified in [\[MS-NLMP\]](#), with the POP3 extensions to NTLM, as specified in [\[MS-OXPOP3\]](#).
- **GSS-API** authentication, as specified in [\[RFC4121\]](#).
- PLAIN authentication, as specified in [\[RFC4616\]](#).
- USER/PASS authentication, as specified in [\[RFC1939\]](#).

C0004:

The specification states: "Once the POP3 server has determined through the use of any authentication command that the client should be given access to the appropriate maildrop, the POP3 server then acquires an exclusive-access lock on the maildrop, as necessary to prevent messages from being modified or removed before the session enters the UPDATE state."

Exchange 2007, Exchange 2010

Once the POP3 server has determined through the use of any authentication command that the client MUST be given access to the appropriate maildrop, the POP3 server makes a snapshot of the list of messages on the maildrop and ignores any additions, changes, or deletes in the maildrop

caused by other Exchange components while the POP session is opened. If a message is deleted while the POP session is opened, the RETR and TOP commands will return an error.

C0005:

The specification states: "After returning a negative status indicator, the server may close the connection."

Exchange 2007, Exchange 2010

After returning a negative status indicator, Exchange Server can close the connection.

2.2.3 [RFC1939] Section 5, STAT Command

V0004:

The specification states: "This memo makes no requirement on what follows the mailbox size. Minimal implementations should just end that line of the response with a CRLF pair. More advanced implementations may include other information."

Exchange 2007, Exchange 2010

Exchange Server does not return any additional information after the mailbox size (in octets).

2.2.4 [RFC1939] Section 5, LIST Command

V0005:

The specification states: "This memo makes no requirement on what follows the message size in the scan listing. Minimal implementations should just end that line of the response with a CRLF pair. More advanced implementations may include other information, as parsed from the message."

Exchange 2007, Exchange 2010

Exchange Server does not return any additional information after the message size (in octets).

2.2.5 [RFC1939] Section 6, QUIT Command

V0006:

The specification states: "If there is an error, such as a resource shortage, encountered while removing messages, the mailbox may result in having some or none of the messages marked as deleted be removed. In no case may the server remove any messages not marked as deleted."

Exchange 2007, Exchange 2010

In the event of an error in the UPDATE phase, Exchange Server is non-atomic in that it does not ensure that all messages marked as deleted are actually removed. There is no case in which Exchange Server removes any messages not marked as deleted.

2.2.6 [RFC1939] Section 7, TOP Command

C0006:

The specification states: "The POP3 commands discussed above must be supported by all minimal implementations of POP3 servers."

Exchange 2007, Exchange 2010

The server MUST support all the commands discussed above.

V0007:

The specification states that the TOP command is an optional POP3 command.

Exchange 2007, Exchange 2010

Exchange POP3 implements the TOP command.

2.2.7 [RFC1939] Section 7, UIDL Command

C0007:

The specification states: "The unique-id of a message is an arbitrary server-determined string, consisting of one to 70 characters in the range 0x21 to 0x7E, which uniquely identifies a message within a maildrop and which persists across sessions."

Exchange 2007, Exchange 2010

Exchange Server uses decimal integers for the unique-id of messages. The unique-ids increase in value but are not necessarily contiguous.

C0008:

The specification states: "The server should never reuse a unique-id in a given maildrop, for as long as the entity using the unique-id exists."

Exchange 2007, Exchange 2010

Exchange Server does not reuse unique-id values, even after a message has been deleted.

C0009:

The specification states: "While it is generally preferable for server implementations to store arbitrarily assigned unique-ids in the maildrop, this specification is intended to permit unique-ids to be calculated as a hash of the message. Clients should be able to handle a situation where two identical copies of a message in a maildrop have the same unique-id."

Exchange 2007, Exchange 2010

Exchange Server uses non-repeating, monotonically increasing decimal numbers as unique-ids; therefore, clients will not encounter two identical copies of a message with the same unique-id. If messages were carried over from an Exchange 2003 server, their unique-ids remain in the Exchange 2003 format, which is different than the format used by Exchange 2007 and Exchange 2010.

2.2.8 [RFC1939] Section 7, USER Command

V0008:

The specification states: "If the POP3 server responds with a negative status indicator ("-ERR") to the USER command, then the client may either issue a new authentication command or may issue the QUIT command."

Exchange 2007, Exchange 2010

Exchange Server does not return a negative status to the USER command because Exchange Server does not verify whether the specified mailbox exists until the client issues the PASS command.

V0009:

The specification states: "The server may return a positive response even though no such mailbox exists."

Exchange 2007, Exchange 2010

As a security precaution, Exchange Server returns a positive status regardless of whether the specified mailbox exists.

V0010:

The specification states: "The server may return a negative response if mailbox exists, but does not permit plaintext password authentication."

Exchange 2007, Exchange 2010

Exchange Server returns a negative response if the mailbox exists, but the server does not permit plaintext password authentication.

2.2.9 [RFC1939] Section 7, PASS Command

C0010:

The specification states: "When the client issues the PASS command, the POP3 server uses the argument pair from the USER and PASS commands to determine if the client should be given access to the appropriate maildrop."

Exchange 2007

If the user is not in the same site as the **CAS** to which the client is connected, Exchange Server sends a login failed error to the user.

V0011:

The specification states: "Since the PASS command has exactly one argument, a POP3 server may treat spaces in the argument as part of the password, instead of as argument separators."

Exchange 2007, Exchange 2010

Exchange Server allows unquoted spaces in the PASS argument, and uses the entire remainder of the command as a single password argument.

2.2.10 [RFC1939] Section 7, APOP Command

V0012:

The specification states that the APOP command is an optional POP3 command.

Exchange 2007, Exchange 2010

Exchange Server does not support the APOP command.

2.2.11 [RFC1939] Section 8, Scaling and Operational Considerations

E0003:

The specification states: "Imposing a per-user maildrop storage quota or the like."

Exchange 2007, Exchange 2010

Exchange Server mailboxes can be configured to have a storage quota. Each user mailbox has a storage quota that is inherited from the storage database configuration. Storage quotas for each mailbox can be changed using the Exchange Management tools.

E0004:

The specification states: "Sites which choose this option should be sure to inform users of impending or current exhaustion of quota, perhaps by inserting an appropriate message into the user's maildrop."

Exchange 2007, Exchange 2010

Exchange Management tools can be used to configure on a per-mailbox basis to warn users that are near their maximum mailbox size.

E0005:

The specification states: "Sites are free to establish local policy regarding the storage and retention of messages on the server, both read and unread. For example, a site might delete unread messages from the server after 60 days and delete read messages after 7 days."

Exchange 2007, Exchange 2010

Exchange Server supports a limited retention policy that can be configured to auto-delete mailbox items based on age. However, this feature is exposed as part of the Exchange storage facility and is not a POP3-specific feature.

2.2.12 [RFC1939] Section 11, Message Format

C0011:

The specification states: "All messages transmitted during a POP3 session are assumed to conform to the standard for the format of Internet text messages [\[RFC822\]](#)."

Outlook 2007, Outlook 2010

All messages transmitted during a POP3 session MUST conform to the standard for the format of Internet text messages [\[RFC822\]](#).

2.2.13 [RFC2449] Section 4, Maximum Length of Command

E0006:

The specification states: "The maximum length of a command is increased from 47 characters (4 character command, single space, 40 character argument, CRLF) to 255 octets, including the terminating CRLF."

Exchange 2007, Exchange 2010

By default, the maximum length of a command is 47 bytes in Exchange Server 2007 and 512 bytes in Exchange Server 2010. The Set-PopSettings cmdlet -MaxCommandSize parameter can be used to set the maximum length of a command in Exchange Server. The minimum size is 40 bytes, the maximum size is 1024 bytes.

2.2.14 [RFC2449] Section 4, Commands Up To 255 Octets

E0007:

The specification states: "Servers which support the CAPA command MUST support commands up to 255 octets. Servers MUST also support the largest maximum command length specified by any supported capability."

Exchange 2007, Exchange 2010

By default, the maximum length of a command is 47 bytes in Exchange Server 2007 and 512 bytes in Exchange Server 2010. The Set-PopSettings cmdlet -MaxCommandSize parameter can be used to set the maximum length of a command in Exchange Server. The minimum size is 40 bytes, the maximum size is 1024 bytes.

2.3 Error Handling

There are no additional error handling considerations beyond what are discussed in sections [2.2.5](#) and [2.2.9](#).

2.4 Security

There are no additional security considerations beyond what are discussed in section [2.2.8](#).

3 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

4 Index

C

[Change tracking](#) 15
[Clarifications - conformance](#) 8
Conformance
 [clarifications](#) 8
 [error handling](#) 14
 [normative variations](#) 7
 [security](#) 14
[Conformance requirements](#) 5

E

[Error handling - conformance](#) 14

G

[Glossary](#) 4

I

[Informative references](#) 5
[Introduction](#) 4

M

[Microsoft implementations](#) 5

N

[Normative references](#) 4
[Normative variations - conformance](#) 7
[Notation](#) 6

R

References
 [informative](#) 5
 [normative](#) 4
Requirements
 [conformance](#) 5

S

[Security - conformance](#) 14

T

[Tracking changes](#) 15