[MS-OXSMTP]:

Simple Mail Transfer Protocol (SMTP) Extensions

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **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 can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets**. Microsoft does not claim any trade secret rights in this documentation.
- **Patents**. Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **License Programs**. To see all of the protocols in scope under a specific license program and the associated patents, visit the Patent Map.
- **Trademarks**. The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names**. The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are 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 as specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications documentation does 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 documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Support. For questions and support, please contact dochelp@microsoft.com.

Preliminary Documentation. This particular Open Specifications document provides documentation for past and current releases and/or for the pre-release version of this technology. This document provides final documentation for past and current releases and preliminary documentation, as applicable and specifically noted in this document, for the pre-release version. Microsoft will release final documentation in connection with the commercial release of the updated or new version of this technology. Because this documentation might change between the pre-release version and the final

version of this technology, there are risks in relying on this preliminary documentation. To the extent that you incur additional development obligations or any other costs as a result of relying on this preliminary documentation, you do so at your own risk.

Revision Summary

Date	Revision History	Revision Class	Comments
4/4/2008	0.1	New	Initial Availability.
6/27/2008	1.0	Major	Initial Release.
8/6/2008	1.01	Minor	Revised and edited technical content.
9/3/2008	1.02	Minor	Updated references.
12/3/2008	1.03	Minor	Updated IP notice.
4/10/2009	2.0	Major	Updated applicable product releases.
7/15/2009	3.0	Major	Revised and edited for technical content.
11/4/2009	3.1.0	Minor	Updated the technical content.
2/10/2010	3.2.0	Minor	Updated the technical content.
5/5/2010	3.3.0	Minor	Updated the technical content.
8/4/2010	4.0	Major	Significantly changed the technical content.
11/3/2010	4.0	None	No changes to the meaning, language, or formatting of the technical content.
3/18/2011	4.1	Minor	Clarified the meaning of the technical content.
8/5/2011	5.0	Major	Significantly changed the technical content.
10/7/2011	5.0	None	No changes to the meaning, language, or formatting of the technical content.
1/20/2012	6.0	Major	Significantly changed the technical content.
4/27/2012	6.1	Minor	Clarified the meaning of the technical content.
7/16/2012	6.1	None	No changes to the meaning, language, or formatting of the technical content.
10/8/2012	7.0	Major	Significantly changed the technical content.
2/11/2013	7.1	Minor	Clarified the meaning of the technical content.
7/26/2013	8.0	Major	Significantly changed the technical content.
11/18/2013	8.0	None	No changes to the meaning, language, or formatting of the technical content.
2/10/2014	8.0	None	No changes to the meaning, language, or formatting of the technical content.
4/30/2014	8.0	None	No changes to the meaning, language, or formatting of the technical content.
7/31/2014	8.0	None	No changes to the meaning, language, or formatting of the technical content.
10/30/2014	8.0	None	No changes to the meaning, language, or formatting of the technical content.

Date	Revision History	Revision Class	Comments
3/16/2015	9.0	Major	Significantly changed the technical content.
5/26/2015	9.0	None	No changes to the meaning, language, or formatting of the technical content.
6/30/2015	10.0	Major	Significantly changed the technical content.
9/14/2015	11.0	Major	Significantly changed the technical content.
6/13/2016	12.0	Major	Significantly changed the technical content.
9/14/2016	12.0	None	No changes to the meaning, language, or formatting of the technical content.
3/16/2017	13.0	Major	Significantly changed the technical content.
7/24/2018	14.0	Major	Significantly changed the technical content.
10/1/2018	15.0	Major	Significantly changed the technical content.
4/7/2021	16.0	Major	Significantly changed the technical content.
4/22/2021	17.0	Major	Significantly changed the technical content.

Table of Contents

1 Introduction

The Simple Mail Transfer Protocol (SMTP) Extensions extend SMTP standards to facilitate authentication negotiation between a client and a server and to enable the server to close connections that exceed configured thresholds.

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

1.1 Glossary

This document uses the following terms:

Augmented Backus-Naur Form (ABNF): A modified version of Backus-Naur Form (BNF), commonly used by Internet specifications. ABNF notation balances compactness and simplicity with reasonable representational power. ABNF differs from standard BNF in its definitions and uses of naming rules, repetition, alternatives, order-independence, and value ranges. For more information, see [RFC5234].

NT LAN Manager (NTLM) Authentication Protocol: A protocol using a challenge-response mechanism for authentication in which clients are able to verify their identities without sending a password to the server. It consists of three messages, commonly referred to as Type 1 (negotiation), Type 2 (challenge) and Type 3 (authentication).

SASL: The Simple Authentication and Security Layer, as described in [RFC2222]. This is an authentication mechanism used by the Lightweight Directory Access Protocol (LDAP).

Simple Mail Transfer Protocol (SMTP): A member of the TCP/IP suite of protocols that is used to transport Internet messages, as described in [RFC5321].

Transmission Control Protocol (TCP): A protocol used with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. TCP handles keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

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

1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the Errata.

1.2.1 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.

[RFC2034] Freed, N., "SMTP Service Extension for Returning Enhanced Error Codes", RFC 2034, October 1996, http://www.rfc-editor.org/rfc/rfc2034.txt

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

[RFC2554] Myers, J., "SMTP Service Extension for Authentication", RFC 2554, March, 1999, http://www.rfc-editor.org/rfc/rfc2554.txt

[RFC3030] Vaudreuil, G., "SMTP Service Extensions for Transmission of Large and Binary MIME Messages", RFC 3030, December 2000, http://www.rfc-editor.org/rfc/rfc3030.txt

[RFC4954] Siemborski, R., and Melnikov, A., Eds., "SMTP Service Extension for Authentication", RFC 4954, July 2007, http://www.rfc-editor.org/rfc/rfc4954.txt

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008, http://rfc-editor.org/rfc/rfc5321.txt

[RFC6531] Yao, J. and Mao, W., "SMTP Extension for Internationalized Email", February 2012, https://tools.ietf.org/html/rfc6531

1.2.2 Informative References

[MS-OXPROTO] Microsoft Corporation, "Exchange Server Protocols System Overview".

[MS-SMTPNTLM] Microsoft Corporation, "NT LAN Manager (NTLM) Authentication: Simple Mail Transfer Protocol (SMTP) Extension".

[MS-XLOGIN] Microsoft Corporation, "Simple Mail Transfer Protocol (SMTP) AUTH LOGIN Extension".

[RFC1870] Klensin, J., Freed, N., Ed., and Moore, K., "SMTP Service Extension for Message Size Declaration", STD 10, RFC 1870, November 1995, http://www.rfc-editor.org/rfc/rfc1870.txt

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002, http://www.rfc-editor.org/rfc/rfc3207.txt

[RFC4409] Gellens, R., and Klensin, J., "Message Submission for Mail", RFC 4409, April 2006, http://www.rfc-editor.org/rfc/rfc4409.txt

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008, http://www.rfc-editor.org/rfc/rfc5322.txt

1.3 Overview

This set of extensions enables additional features and communication between an **SMTP** client and server.

These extensions define the relaxed AUTH command extension, which extends [RFC4954] to provide an alternative response format for the first server challenge which allows the server to verify that it supports the requested **Simple Authentication and Security Layer (SASL)** mechanism.

These extensions define scenarios where the server can close connections that are consuming too many resources.

The SMTPUTF8 extension defines transport and delivery of email messages with internationalized addresses or headers, which is an extension to [RFC6531].

1.4 Relationship to Other Protocols

The SMTP Extensions extend [RFC6531], [RFC5321], [RFC4954], and other related extensions.

The Relaxed AUTH Command Extension is used with **SASL** mechanisms, such as the NT LAN Manager (NTLM) Authentication: Simple Mail Transfer Protocol (SMTP) Extension specified in [MS-SMTPNTLM], that require the client to provide an initial response before the server can issue a challenge.

For conceptual background information and overviews of the relationships and interactions between this and other protocols, see [MS-OXPROTO].

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

The SMTP Extensions are applicable to scenarios in which clients will be authenticating to and submitting email messages directly to a server. This specification does not cover how **SMTP** transport agents affect or alter messages on the server.

1.7 Versioning and Capability Negotiation

The SMTP Extensions introduce no new versioning mechanisms beyond those that exist in **SMTP**, as described in [RFC5321] and [RFC6531].

Negotiation of SMTP options is specified in [RFC5321] section 4.1.1.1, [RFC6531] section 3.2.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

The transport of the protocol that the SMTP Extensions extend is specified in [RFC5321] section 1.1, and the SMTP Extension for supporting internationalized email address is specified in [RFC6531].

2.2 Message Syntax

The syntax of the messages that are exchanged between the client and the server are specified in [RFC5321] and [RFC6531].

2.2.1 SASL_Mechanism_Supported

The **SASL_Mechanism_Supported** message is used in place of a server challenge that contains no data, as specified in [RFC4954] section 4. The format of this message is specified by the following **Augmented Backus-Naur Form (ABNF)** notation.

```
mechanism_supported = "334" SP mechanism SP "supported"
mechanism           = 1*20 mech_char
mech_char           = %x41-5A / %x30-39 / %x2D / %x5F
```

The value of the mechanism ABNF rule is equal to the mechanism argument passed in the **AUTH** command by the client.

3 Protocol Details

3.1 Client Details

The client role MUST conform to [RFC5321] and for the exchange of messages with the server. The client role MUST conform to the SMTP Service Extension for Authentication specified in [RFC2554] and SHOULD<1> conform to SMTP Service Extension for Authentication specified in [RFC4954]. Throughout this section, SMTP Service Extension for Authentication refers to whichever version of the SMTP Service Extension for Authentication that the client supports.

When supporting email addresses in internationalized forms, the client role MUST conform to [RFC6531].

3.1.1 Abstract Data Model

The client state model is specified in [RFC5321], with the additions in the SMTP Service Extension for Authentication.

3.1.2 Timers

None beyond what is specified in [RFC5321], with the additions in the SMTP Service Extension for Authentication.

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

Except as specified in section 3.1.5.1, the client MUST conform to [RFC5321], with the additions in the SMTP Service Extension for Authentication, for all message processing events and sequencing rules.

3.1.5.1 Receiving a SASL_Mechanism_Supported Message

When a client receives a **SASL_Mechanism_Supported** message, as specified in section 2.2.1, the client MUST verify that it sent an **AUTH** command with an initial-response. The client MAY also validate that the message contains the mechanism it sent in the **AUTH** command and fail the communication if such verification failed.

The client MUST then continue negotiation by sending a client response to the server with the content specified by the client's implementation of the negotiated **SASL** mechanism, as specified in the SMTP Service Extension for Authentication.

3.1.6 Timer Events

None beyond what is specified in [RFC5321], with the additions in the SMTP Service Extension for Authentication.

3.1.7 Other Local Events

None.

3.2 Server Details

The server role MUST conform to [RFC5321] for the exchange of messages with the client. The server role MUST conform to the SMTP Service Extension for Authentication specified in [RFC2554] and SHOULD<2> conform to the SMTP Service Extension for Authentication specified in [RFC4954]. Throughout this section, SMTP Service Extension for Authentication refers to whichever version of the SMTP Service Extension for Authentication that the server supports.

The SMTP extension to support internationalized email addresses is specified in [RFC6531].

3.2.1 Abstract Data Model

The server state model is specified in [RFC5321], with the addition in the SMTP Service Extension for Authentication.

3.2.2 Timers

ConnectionTimer: A timer that identifies how much time has elapsed since a session was initiated.

ConnectionInactivityTimer: A timer that identifies how much time has elapsed since a client provided input. This timer is corresponds to the server time-out specified in [RFC5321] section 4.5.3.2.7.

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

Except as specified in section 3.2.5.1, the server role MUST be compliant with the message processing and sequencing rules that are specified in [RFC5321], with the additions in the SMTP Service Extension for Authentication.

When supporting email addresses in internationalized forms, the server role MUST conform with [RFC6531].

3.2.5.1 Sending a SASL_Mechanism_Supported Message

When the server receives an **AUTH** command that does not include the optional initial response, as specified in [RFC4954] section 4, and the specified **SASL** mechanism provides an empty server string to include in the server challenge, the server SHOULD respond with a **SASL_Mechanism_Supported** message, as specified in section 2.2.1.

3.2.6 Timer Events

The **ConnectionTimeOut** timer event occurs when the **ConnectionTimer**, as specified in section 3.2.2, expires. The server MUST end the session as specified in [RFC5321] section 3.8.

The **ConnectionInactivityTimeOut** timer event occurs when the **ConnectionInactivityTimer**, as specified in section 3.2.2, expires. The server MUST end the session as specified in [RFC5321] section 3.8.

3.2.7 Other Local Events

ConnectionEstablished event: Occurs when a **TCP** connection is established to the server on the configured **SMTP** port. The server MUST initialize a **ConnectionTimer**, as specified in section 3.2.2, for each connection. If the server is a gateway server, as specified in [RFC5321] section 2.3.10, the **ConnectionTimer** MUST be set to 5 minutes. If the server is a relay server, as specified in [RFC5321] section 2.3.10, the **ConncectionTimer** MUST be set to 10 minutes. The server MUST initialize a **ConnectionInactivityTimer**, as specified in section 3.2.2, for each connection. The **ConnectionInactivityTimer** is set to a value configured by the administrator.

CommandReceived event: Occurs when the server receives a command from the client. The server MUST reset the **ConnectionInactivityTimer** associated with the client's TCP connection to the timeout value configured by the administrator.

MaxHopCount event: Occurs when the number of **Received** header fields, as specified in [RFC5321] section 6.3, exceeds the configured maximum. The SMTP response code MUST indicate a permanent failure, as specified in [RFC5321] section 4.2.1. This response is sent at the end of a **DATA** command, as specified in [RFC5321] section 4.1.1.4, or a **BDAT** command, as specified in [RFC3030].

MaxLocalHopCount event: Occurs when the server has received the message more than the configured maximum number of times. The SMTP response code MUST indicate a permanent failure, as specified in [RFC5321] section 4.2.1. This response is sent at the end of a **DATA** or **BDAT** command.

TooManyRecipients event: Occurs when the number of recipients exceeds the configured maximum. The SMTP response code MUST indicate a transient failure, as specified in [RFC5321] section 4.2.1. This response MUST be sent at the end of a **RCPT TO** command, as specified in [RFC5321] section 4.1.1.3.

MessageRateLimitExceeded event: Occurs when the message submission rate for a client has exceeded the configured limit. The SMTP response code MUST be 421, as specified in [RFC5321] section 4.2.2, and the enhanced status code, as specified in [RFC2034], MUST be 4.4.2. This response MUST be sent at the end of a **MAIL FROM** command, as specified in [RFC5321] section 4.1.1.2. The server MUST end the session.

HeaderSizeExceeded event: Occurs when the message header size exceeds the configured size limit. The SMTP response code MUST be 552 and the enhanced status code MUST be 5.3.4. This response MUST be sent at the end of a **DATA** or **BDAT** command.

MessageSizeExceeded event: Occurs when the message size exceeds the configured size limit. The SMTP response code MUST be 552 and the enhanced status code MUST be 5.3.4. This response MUST be sent at the end of a **DATA** or **BDAT** command.

ProtocolViolationCount event: Occurs when the configured maximum number of logon or protocol errors is exceeded. The SMTP response code MUST be 421 and the enhanced status code MUST be 4.7.0. The server MUST end the session.

OutOfResources event: Occurs when a client initiates a TCP connection to the server and the server is low on memory or disk space. The SMTP response code MUST be 452 and the enhanced status code MUST be 4.3.1.

NewConnectionNotAvailable event: Occurs when an SMTP server cannot process a new connection. It indicates that the process has stopped responding or is in a crashed condition. The SMTP response code MUST be 421 and the enhanced status code MUST be 4.4.2. The server MUST end the session.

BindingNotConfigured event: Occurs when an SMTP server is not configured to accept connections from a client at a specific IP address or from the specific user. The SMTP response code MUST be 421 and the enhanced status code MUST be 4.3.2. The server MUST end the session.

ConnectionCountExceeded event: Occurs when an SMTP server has exceeded the configured maximum concurrent inbound connections. The SMTP response code MUST be 421 and the enhanced status code MUST be 4.3.2. The server MUST end the session.

ConnectionCountPerSource event: Occurs when an SMTP server has exceeded the configured limit on inbound connections for an IP address. The SMTP response code MUST be 421 and the enhanced status code MUST be 4.3.2. The server MUST end the session.

IPAddressNotAllowed event: Occurs when a gateway SMTP server binding receives a connection from an IP address that the server has been configured to not accept connections from. The SMTP response code MUST be 550 and the enhanced status code MUST be 5.7.1.

AcknowledgementDelay event: Occurs when the server waits longer than the configured time limit for a mail item to be delivered to the next hop. This event occurs after the end of **DATA** or **BDAT LAST** command, as specified in [RFC3030] section 2. If the **AcknowledgementDelay** event occurs, the server MUST send acknowledgment of receiving the mail item even if transport has not delivered the item to the next hop. The server sends the response as specified in [RFC5321] and processes the next command. The server state does not change.

Tarpit event: Occurs at the end of a command when the server sends an error message to an unauthenticated user, and once again if the same client connects to the server. The server MUST ignore connection attempts for 5 seconds and then send the response to the client. The server sends the response as specified in [RFC5321] and processes the next command. The server state does not change.

4 Protocol Examples

The following sequence diagram shows an example of an authentication exchange that uses the **SASL_Mechanism_Supported** message described in section 2.2.1. In this example, the client requests authentication using the NT LAN Manager (NTLM) Authentication: Simple Mail Transfer Protocol (SMTP) Extension, as described in [MS-SMTPNTLM].

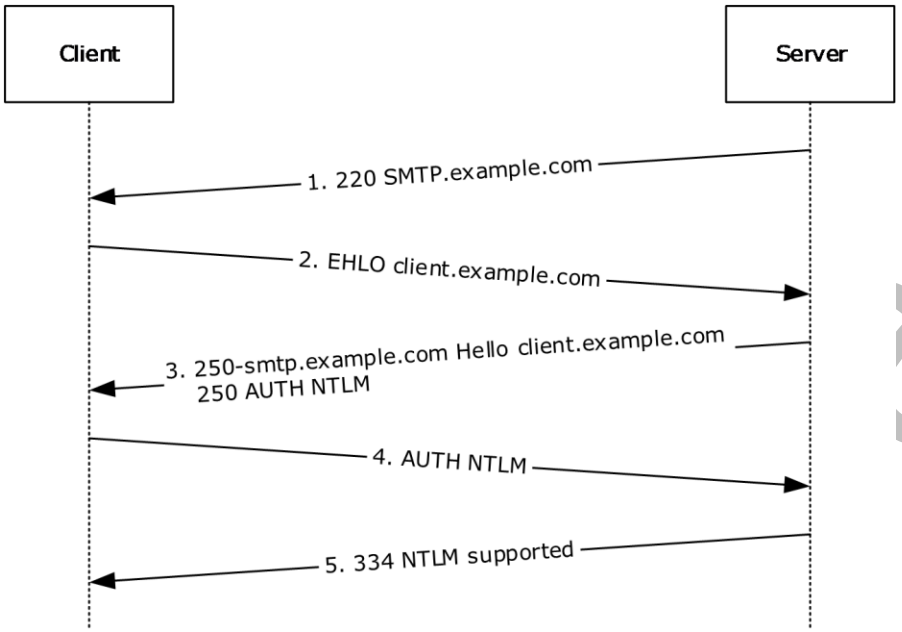

Figure 1: Example authentication exchange

1. The initial response by the **SMTP** server ("220 SMTP.example.com") is the greeting by the server as specified in [RFC5321].
2. The client sends the **EHLO** command.
3. The server responds with, among other things, an indication of support for **NTLM** authentication.
4. The client issues the **AUTH** NTLM command, omitting the initial response.
5. The server responds with the **SASL_Mechanism_Supported** message.

5 Security

5.1 Security Considerations for Implementers

Security considerations are described in [RFC1870] section 9, [RFC2034] section 7, [RFC3207] section 6, [RFC4409] section 9, [RFC4954] section 9, [RFC5321] section 7, [RFC5322] section 5, [RFC6531] section 5, [MS-SMTPNTLM], and [MS-XLOGIN] section 5.1.

5.2 Index of Security Parameters

Security parameters for message submission authentication are described in [RFC4409].

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include updates to those products.

- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Office Outlook 2003
- Microsoft Office Outlook 2007
- Microsoft Outlook 2010
- Microsoft Outlook 2013
- Microsoft Outlook 2016
- Microsoft .NET Framework 2.0
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5
- Microsoft .NET Framework 4.7
- Microsoft .NET Framework 4.8
- Windows 2000 Professional operating system
- Windows XP operating system
- Windows Vista operating system
- Windows 7 operating system
- Windows 8 operating system
- Windows 8.1
- Windows 10 operating system
- Windows 2000 Server operating system
- Windows Server 2003 operating system
- Windows Server 2008 operating system
- Windows Server 2012 operating system
- Windows Server 2012 R2
- Windows Server 2016 operating system

- Windows Server 2019 operating system
- Windows Server 2022 operating system
- Microsoft Exchange Server 2019
- Microsoft Outlook 2019
- Microsoft Outlook 2021

Exceptions, if any, are noted in this section. If an update version, service pack or Knowledge Base (KB) number appears with a product name, the behavior changed in that update. The new behavior also applies to subsequent updates unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms "SHOULD" or "SHOULD NOT" implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term "MAY" implies that the product does not follow the prescription.

<1> Section 3.1: Windows 2000 Professional, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2012, and Windows Server 2012 R2 do not conform to [RFC4954].

<2> Section 3.2: Windows 2000 Professional, Windows XP, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2012, and Windows Server 2012 R2 do not conform to [RFC4954].

7 Change Tracking

This section identifies changes that were made to this document since the last release. Changes are classified as Major, Minor, or None.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements.
- A document revision that captures changes to protocol functionality.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **None** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the relevant technical content is identical to the last released version.

The changes made to this document are listed in the following table. For more information, please contact dochelp@microsoft.com.

Section	Description	Revision class
6 Appendix A: Product Behavior	Updated list of supported products.	major

8 Index