[MS-OXSMTP]:
Simple Mail Transfer Protocol (STMP) Mail Submission Extensions Specification

Revision Summary

Date	Revision History	Revision Class	Comments
04/04/2008	0.1		Initial Availability.
06/27/2008	1.0		Initial Release.
08/06/2008	1.01		Revised and edited technical content.
09/03/2008	1.02		Updated references.
12/03/2008	1.03		Updated IP notice.
04/10/2009	2.0		Updated applicable product releases.
07/15/2009	3.0	Major	Revised and edited for technical content.

Table of Contents

1   Introduction

The **Simple Mail Transport Protocol (SMTP)** Message Submission for Mail protocol, as specified in [RFC4409], profiles SMTP mechanisms specified in [RFC2821] and others to provide mail submission mechanisms for client mail systems. SMTP was originally defined to provide for mail transfer between mail servers. It is now widely used as a message submission mechanism, where client messaging systems introduce new messages into the mail routing network.

This specification profiles [RFC4409], identifying the elements necessary to conform to Exchange Server protocols.

1.1   Glossary

The following terms are defined in [MS-OXGLOS]:

> **Mail User Agent (MUA)**
> **Simple Mail Transfer Protocol (SMTP)**

The following terms are specific to this document:

> **Message Submission Agent (MSA):** A process that accepts messages from a Mail User Agent (MUA) and either delivers it or acts as a Simple Mail Transfer Protocol (SMTP) client to submit the messages to a Message Transfer Agent (MTA).

> **Message Transfer Agent (MTA):** An SMTP server that accepts mail from a Mail Submission Agent (MSA) or another MTA and delivers the mail or relays it to another MTA.

> **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   References

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. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

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

[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.

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

1.2.2   Informative References

[RFC2821] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001, http://www.ietf.org/rfc/rfc2821.txt.

[RFC821] Postel, J., "Simple Mail Transfer Protocol", RFC 821, August 1982, http://www.ietf.org/rfc/rfc821.txt.

Release: Sunday, July 12, 2009

1.3 Protocol Overview

[RFC4409] describes a profile of SMTP [RFC2821] and others that defines how clients submit mail to a server. This document specifies which parts of [RFC4409] are necessary for message submission.

1.4 Relationship to Other Protocols

This specification profiles [RFC4409] to define the protocol for message submission. [RFC4409] is based on SMTP as specified in [RFC2821].

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

This protocol is applicable to scenarios where clients will be submitting e-mail messages directly to a server.

1.7 Versioning and Capability Negotiation

This specification introduces no new versioning mechanisms beyond those that exist in SMTP.

Negotiation of SMTP options is part of [RFC4409]. The EHLO response indicates what capabilities are present on the server.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

None.

2.2 Message Syntax

None.

3   Protocol Details

This protocol describes the process for a client submitting e-mail messages to a **Message Transfer Agent (MTA)**. In [RFC4409], three components are described to represent the interaction: a **Mail User Agent (MUA)**, a **Message Submission Agent (MSA)**, and an MTA. These components describe an architecture, shown in Figure 1, where the MUA creates the message, the MSA picks it up and, via SMTP, submits it to the MTA for transmission to the recipient.
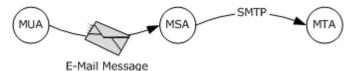

Figure 1: Message transmission

Most modern e-mail clients combine the MUA and the MSA, such that there is no perceptible handoff between the MUA and MSA functions. As a result, the MSA provides SMTP client capabilities while the MTA provides the SMTP server capabilities. This protocol only covers the path between the MSA and the MTA. Thus the profile of [RFC4409] provided is broken into two roles — the client and the server — where the client performs SMTP submissions and the server accepts the SMTP submissions. Aspects of [RFC4409] that describe the interaction between the MUA and the MSA are specifically excluded from this protocol.

3.1   Client Details

The MUA/MSA process is the client. The MUA functionality is used to acquire or create the message and the MSA functionality performs an SMTP client submission. The client, therefore, only acts as an SMTP client; it does not have the ability to receive **messages** via SMTP as an SMTP server.

The client protocol for message submission conforms to [RFC4409] except as identified in the following table.

Section	Description
3.1	The client SHOULD submit messages on port 587, port 25 or any port that a site chooses for message submission.
3.2	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
3.3	The client SHOULD authenticate using mechanisms defined in [RFC2554]. The client SHOULD use AUTH LOGIN or AUTH **NTLM**.
4.1	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
4.2	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
4.3	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
5.1	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
5.2	This section is not included in the client profile because the MUA and MSA functionality are

Section	Description
	integrated into the same process.
6	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
7	The client SHOULD support DSN, AUTH, and STARTTLS. AUTH SHOULD be supported as specified in section 3.3 of this table.
8	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.

3.1.1 Abstract Data Model

None.

3.1.2 Timers

None.

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

None.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 Server Details

The server component of Message submission conforms to [RFC4409] except as identified in the following **table**.

Section	Description
3.1	The server SHOULD allow messages to be submitted on **port** 587, port 25, or any port that a site chooses for Message submission.
3.2	The server SHOULD offer authenticate mechanisms as defined in [RFC2554].
3.3	The server SHOULD offer authenticate mechanisms as defined in [RFC2554]. The client SHOULD offer AUTH LOGIN or AUTH NTLM.

Section	Description
4.1	The server SHOULD respond with a 550 or a 554 for error **conditions**.
4.2	The server SHOULD respond with a 550 or a 554 for error conditions.
4.3	The server SHOULD require client authentication. If the server does not require client authentication, the server MUST NOT issue an error response to an unauthenticated MAIL command.
7	The server SHOULD implement DSN, AUTH, and STARTTLS. The server SHOULD offer AUTH LOGIN and AUTH NTLM.

3.2.1 Abstract Data Model

None.

3.2.2 Timers

None.

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

None.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4   Protocol Examples

None.

5   Security

5.1   Security Considerations for Implementers

None.

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 product versions:

- Microsoft Office Outlook 2003

- Microsoft Exchange Server 2003

- Microsoft Office Outlook 2007

- Microsoft Exchange Server 2007

- Microsoft Outlook 2010

- Microsoft Exchange Server 2010

Exceptions, if any, are noted below. If a service pack number appears with the product version, behavior changed in that service pack. The new behavior also applies to subsequent service packs of the product unless otherwise specified.

Unless otherwise specified, any statement of optional behavior in this specification 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.

7 Change Tracking

This section will report content and/or editorial changes, beginning with the next release.

8 Index

C

Change tracking

E

Examples - overview

G

Glossary

I

Informative references
Introduction

M

Messages
  overview

N

Normative references

O

Overview (synopsis)

P

Preconditions
Prerequisites
Product behavior

R

References
  informative
  normative
Relationship to other protocols

S

Security
  overview

T

Tracking changes