[MS-XLOGIN]:
SMTP Protocol AUTH LOGIN Extension Specification

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 iplg@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.

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.

Copyright © 2008 Microsoft Corporation.

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.

Copyright © 2008 Microsoft Corporation.

Table of Contents

Copyright © 2008 Microsoft Corporation.

1 Introduction

This document specifies an authentication mechanism that is provided through the **SMTP** Service Extension for Authentication [RFC4954] called AUTH LOGIN.

1.1 Glossary

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

Secure Sockets Layer (SSL)
Simple Mail Transfer Protocol (SMTP)

The following terms are specific to this document:

Transport Layer Security (TLS): A security protocol that supports confidentiality and integrity of messages in client and server applications communicating over open networks. TLS supports server and, optionally, client authentication by using X.509 certificates [X509]. TLS is standardized in the IETF TLS working group.

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.

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

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006, http://www.ietf.org/rfc/rfc4648.txt.

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

[X509] ITU-T, "Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks", Recommendation X.509, August 2005, http://www.itu.int/rec/T-REC-X.509/en.

1.2.2 Informative References

[RFC4346] Dierks, T. and Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006, http://www.ietf.org/rfc/rfc4346.txt.

Copyright © 2008 Microsoft Corporation.

[SSL] Frier, A., Karlton, P., and Kocher, P., "The SSL Protocol Version 3.0", November 1996, http://wp.netscape.com/eng/ssl3/draft302.txt.

1.3 Protocol Overview

Client applications that connect to the SMTP service can use a number of different authentication mechanisms. The SMTP Service Extension for Authentication [RFC4954] defines a service extension to SMTP as specified in [RFC2821], where a client SHOULD specify an authentication method to the server. AUTH LOGIN is one such authentication protocol for SMTP.

1.4 Relationship to Other Protocols

This specification defines an implementation of a protocol using [RFC4954].

1.5 Prerequisites/Preconditions

All prerequisites and preconditions are specified in [RFC2821] and [RFC4954].

1.6 Applicability Statement

This protocol extension does not change the way that [RFC4954] is used.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

Copyright © 2008 Microsoft Corporation.

2 Messages

The following sections specify the AUTH LOGIN **Message** syntax and how they are transported.

2.1 Transport

This protocol extension does not change the base transport specified by [RFC 4954].

2.2 Message Syntax

2.2.1 EHLO Response

Server support for the AUTH LOGIN extension is identified in the EHLO response per [RFC4954] section 3. For example:

```
S: 220 SMTP.example.com
C: EHLO client.example.com
S: 250-smtp.example.com  Hello client.example.com
S: 250 AUTH LOGIN
```

The server response of AUTH LOGIN as part of the responses to EHLO indicates support for AUTH LOGIN.

2.2.2 User Name and Password Values

The AUTH LOGIN extension transmits two values as part of the Message sequence: a user name and a password. Each of these values is encoded using base64 per [RFC4648] before being transmitted. The values, before encoding, are defined as follows:

```
USERNAME = 1*CHAR
PASSWORD = 1*CHAR
```

2.2.3 AUTH LOGIN Command

Support for LOGIN authentication is through the AUTH command, as specified in [RFC4954] section 4. There are two forms for requesting LOGIN authentication, as specified in the following sections.

2.2.3.1 Simple AUTH LOGIN

To request LOGIN authentication, the client issues the AUTH command with the parameter LOGIN (AUTH_LOGIN_COMMAND):

```
AUTH LOGIN<CR><LF>
```

If AUTH LOGIN is not supported, then the server responds with a 504 error Message as specified in [RFC4954] section 4.

If AUTH LOGIN is supported on the server, then the server responds with the AUTH_LOGIN_Username_Challenge:

```
334 VXNlcm5hbWU6<CR><LF>
```


Copyright © 2008 Microsoft Corporation.

The client then responds with the user name to be used for authentication, base64-encoded as specified in [RFC4648]. For example, if the client's user name was "Charlie", then the client would respond with the following Login_Username_Response:

```
Q2hhcmxpZQ==<CR><LF>
```

The server then responds with the AUTH_LOGIN_Password_Challenge:

```
334 UGFzc3dvcmQ6<CR><LF>
```

The client then responds with the password to be used for authentication, base64-encoded as specified in [RFC4648]. For example, if the client's password was "password", then the client would respond with the following Login_Username_Response:

```
cGFzc3dvcmQ=<CR><LF>
```

If the authentication is successful, then the server issues a LOGIN_Succeeded_Response or a LOGIN_Failed_Response, corresponding to a 235 reply for success or a 535 reply for a failure [RFC4954].

2.2.3.2 AUTH LOGIN with User Name

To request LOGIN authentication, the client issues the AUTH command with the parameter LOGIN and the user name to be used for authentication, base64-encoded as specified in [RFC4648]. For example, if the client's user name was "Charlie", then the client would initiate AUTH LOGIN as follows (AUTH_LOGIN_COMMAND_USER):

```
AUTH LOGIN Q2hhcmxpZQ==<CR><LF>
```

If AUTH LOGIN is not supported, then the server responds with a 504 error Message as specified in [RFC4954] section 4.

If AUTH LOGIN is supported on the server, then the server responds with the AUTH_LOGIN_Password_Challenge:

```
334 UGFzc3dvcmQ6<CR><LF>
```

The client then responds with the password to be used for authentication, base64-encoded as specified in [RFC4648]. For example, if the client's password was "password", then client would respond with the following Login_Username_Response:

```
cGFzc3dvcmQ=<CR><LF>
```

If the authentication is successful, then the server issues a LOGIN_Succeeded_Response or a LOGIN_Failed_Response, corresponding to a 235 reply for success or a 535 reply for a failure [RFC4954].

Copyright © 2008 Microsoft Corporation.

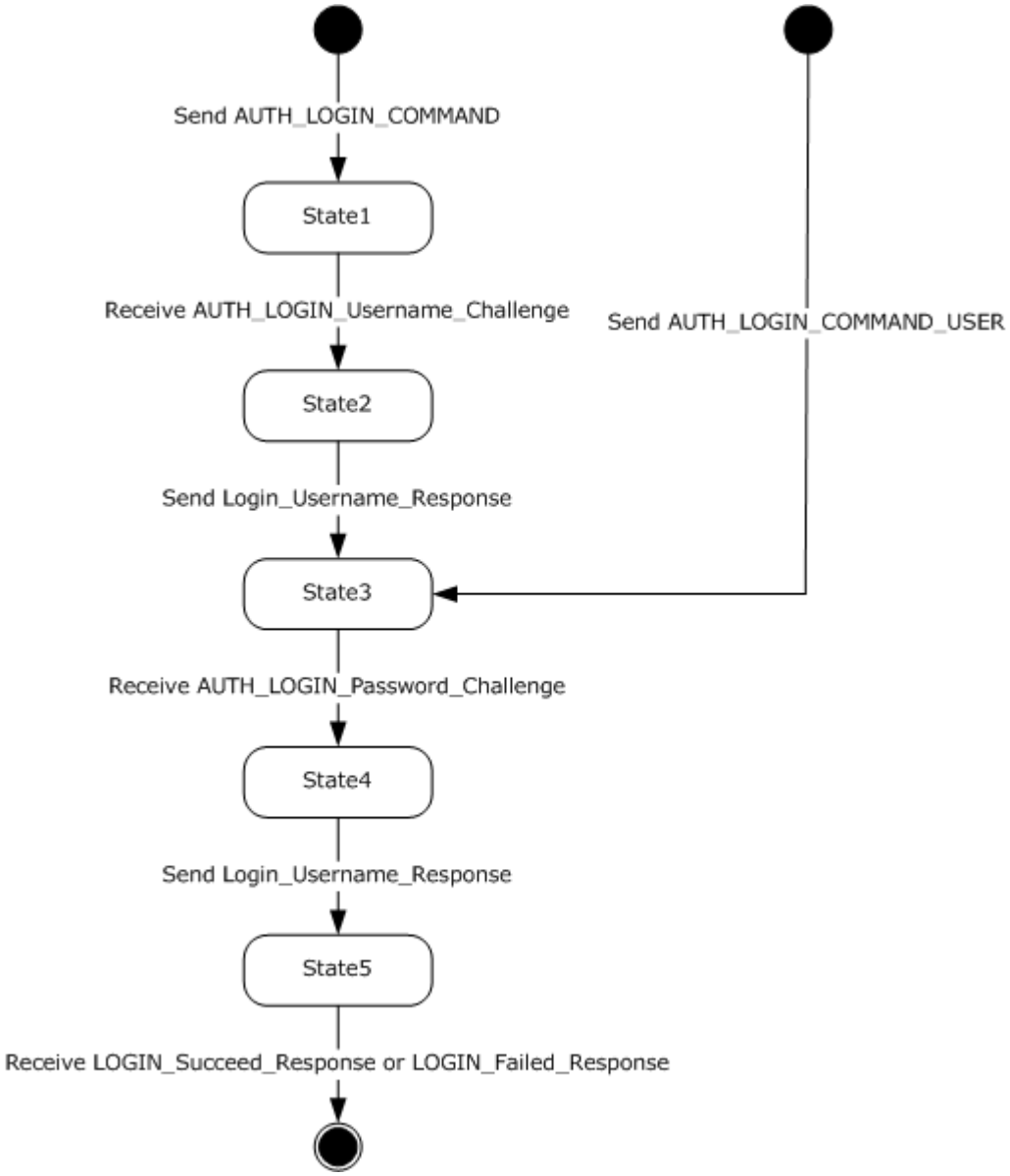
3 Protocol Details

The following sections specify details of the AUTH LOGIN protocol extension, including abstract data models and Message processing **rules**.

3.1 Common Details

3.1.1 Abstract Data Model

The abstract data model shown in Figure 1 represents the sequence of messages described in the previous section.



Copyright © 2008 Microsoft Corporation.

Figure 1: Abstract data model

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

This protocol does not change Message processing **events** or sequencing rules of messages beyond that which is specified in [RFC4954].

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

Copyright © 2008 Microsoft Corporation.

4 Protocol Example

Following is an example of the use of the AUTH LOGIN protocol extension. The example demonstrates SMTP authentication using the AUTH LOGIN protocol.

```
S: 220 SMTP.example.com
C: EHLO client.example.com
S: 250-smtp.example.com  Hello client.example.com
S: 250 AUTH LOGIN
C: AUTH LOGIN
S: 334 VXNlcm5hbWU6
C: Q2hhcmxpZQ==
S: 334 UGFzc3dvcmQ6
C: cGFzc3dvcmQ=
S: 235 authentication successful
```

In this example, a client connects to an SMTP server. The initial response by the server ("220 SMTP.example.com") is the greeting by the server. The client responds with the EHLO command, which is required to activate the extended command set. The server responds with, among other things, an indication of support for AUTH LOGIN. The client then issues the AUTH LOGIN command. The server responds with the first base64-encoded challenge. The client responds with "W2hhcmxpZQ==", which is the base64-encoded name "Charlie". The server then issues the second base64-encoded challenge and the client response with "cGFzc3dvcmQ=", which is the base64-encoded password "password". Successful authentication then results in a server response of "235".

Copyright © 2008 Microsoft Corporation.

5 Security

5.1 Security Considerations for Implementers

This protocol offers no inherent security mechanisms to protect the user credentials during authentication. Because of this, it is extremely important to only use this protocol when also using a secure communication channel such as SSL or **TLS**. Even when using SSL or TLS, the authentication credentials are available to the SMTP server, where it is possible that they could be recorded for future use. The recommendation, therefore, is to not use this protocol except in circumstances where no other option is available.

In environments where the use of TLS or other external security is mandated, the AUTH LOGIN advertisement SHOULD be suppressed until a secure channel is negotiated. TLS in particular exhibits this behavior where the SMTP session is restarted after TLS is negotiated. For more information, see [RFC4346].

5.2 Index of Security Parameters

None.

Copyright © 2008 Microsoft Corporation.

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.

Copyright © 2008 Microsoft Corporation.

7 Change Tracking

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

Copyright © 2008 Microsoft Corporation.

8 Index

Copyright © 2008 Microsoft Corporation.