[MS-OXLDAP]:
Lightweight Directory Access Protocol (LDAP) Version 3 Extensions

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 Open Specification Promise or the Community Promise. 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.
- **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.

Preliminary Documentation. This Open Specification provides documentation for past and current releases and/or for the pre-release (beta) version of this technology. This Open Specification is final documentation for past or current releases as specifically noted in the document, as applicable; it is preliminary documentation for the pre-release (beta) versions. Microsoft will release final documentation in connection with the commercial release of the updated or new version of this technology. As the documentation may change between this preliminary version and the final version of this technology, there are risks in relying on 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
04/04/2008	0.1		Initial Availability.
04/25/2008	0.2		Revised and updated property names and other technical content.
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 technical content for new product releases.
07/15/2009	3.0	Major	Revised and edited for technical content.
11/04/2009	4.0.0	Major	Updated and revised the technical content.
02/10/2010	4.1.0	Minor	Updated the technical content.
05/05/2010	4.1.1	Editorial	Revised and edited the technical content.
08/04/2010	4.2	Minor	Clarified the meaning of the technical content.
11/03/2010	4.2	No change	No changes to the meaning, language, or formatting of the technical content.
03/18/2011	4.3	Minor	Clarified the meaning of the technical content.
08/05/2011	5.0	Major	Significantly changed the technical content.
10/07/2011	5.0	No change	No changes to the meaning, language, or formatting of the technical content.
01/20/2012	6.0	Major	Significantly changed the technical content.

Table of Contents

1 Introduction 5
1.1 Glossary 5
1.2 References 5
1.2.1 Normative References 5
1.2.2 Informative References 6
1.3 Overview 6
1.4 Relationship to Other Protocols 7
1.5 Prerequisites/Preconditions 7
1.6 Applicability Statement 7
1.7 Versioning and Capability Negotiation 7
1.8 Vendor-Extensible Fields 7
1.9 Standards Assignments 7

2 Messages 8
2.1 Transport 8
2.2 Message Syntax 8
2.2.1 Extension-Specific Name Attributes 10
2.2.1.1 Display Name 10
2.2.2 Extension-Specific Organizational Attributes 10
2.2.2.1 Organizational Unit 10
2.2.2.2 Reports 10
2.2.3 Extension-Specific E-Mail Attributes 10
2.2.3.1 Account 10
2.2.3.2 Exchange Distinguished Name 10
2.2.3.3 Exchange Home Server 10
2.2.3.4 Proxy Addresses 11
2.2.3.5 X.400 Address 11
2.2.4 Extension-Specific Telephone Attributes 11
2.2.4.1 Assistant Phone Number 11
2.2.4.2 Secondary Phone Number 11
2.2.5 Other Extension-Specific Attributes 11
2.2.5.1 Object Class 11
2.2.5.2 S/MIME Certificate 12

3 Protocol Details 13
3.1 Client Details 13
3.1.1 Abstract Data Model 13
3.1.2 Timers 13
3.1.3 Initialization 13
3.1.3.1 Querying for Supported Controls 13
3.1.3.2 Querying for Supported Capabilities 13
3.1.4 Higher-Layer Triggered Events 13
3.1.5 Message Processing Events and Sequencing Rules 14
3.1.5.1 Issuing a Search Request 14
3.1.5.1.1 Retrieving a Search Base 14
3.1.5.1.2 Basic Search Filter 15
3.1.5.1.3 Advanced Search Filter 15
3.1.5.1.4 ANR Search Filter 16
3.1.5.1.5 Virtual List View Search Filter 16
3.1.6 Timer Events 16

3.1.7 Other Local Events 16
3.2 Server Details 16
3.2.1 Abstract Data Model 16
3.2.2 Timers 16
3.2.3 Initialization 17
3.2.4 Higher-layer Triggered Events 17
3.2.5 Message Processing Events and Sequencing Rules 17
3.2.5.1 Handling a Query for the supportedControl Attribute 17
3.2.5.2 Handling a Query for the supportedCapabilities Attribute 17
3.2.5.3 Handling Search Requests 17
3.2.5.3.1 Handling a Query for the defaultNamingContext Attribute 17
3.2.5.3.2 Responding to Query Attributes 17
3.2.6 Timer Events 18
3.2.7 Other Local Events 18

4 Protocol Examples 19
4.1 Simple Search Scenario 19

5 Security 21
5.1 Security Considerations for Implementers 21
5.2 Index of Security Parameters 21

6 Appendix A: Product Behavior 22

7 Change Tracking 24

8 Index 26

1 Introduction

The Lightweight Directory Access Protocol (LDAP) Version 3 Extensions is a set of extensions to **LDAP**, as described in [RFC4511] and [RFC4512], and the LDAP user schema, as described in [RFC4519], that defines new attributes and values for existing attributes related to the operation of e-mail clients and servers.

Sections 1.8, 2, and 3 of this specification are normative and contain RFC 2119 language. Sections 1.5 and 1.9 are also normative but cannot contain RFC 2119 language. All other sections and examples in this specification are informative.

1.1 Glossary

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

ambiguous name resolution (ANR)
Augmented Backus-Naur Form (ABNF)
distinguished name (DN)
LDAP
object identifier (OID)

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

mailbox
public folder
recipient
S/MIME (Secure/Multipurpose Internet Mail Extensions)
Simple Mail Transfer Protocol (SMTP)

The following terms are specific to this document:

AD-type server: An LDAP server that returns an object identifier (OID) value of "1.2.840.113556.1.4.800" when it is queried for the supportedCapabilities LDAP attribute.

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

References to Microsoft Open Specification documents do not include a publishing year because links are to the latest version of the documents, which are updated frequently. References to other documents include a publishing year when one is available.

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.

[LDAPEX-SVB] Boreham, D., Sermersheim, J., and Kashi, A., "LDAP Extensions for Scrolling View Browsing of Search Results", Internet-Draft <draft-ietf-ldapext-ldapv3-vlv-09.txt>, November 2002, http://www.ietf.org/proceedings/02nov/I-D/draft-ietf-ldapext-ldapv3-vlv-09.txt

[MS-OXOABK] Microsoft Corporation, "Address Book Object Protocol Specification".

[RFC1274] Barker, P., and Kille, S., "The COSINE and Internet X.500 Schema", RFC 1274, November 1991, http://www.ietf.org/rfc/rfc1274.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

[RFC2696] Weider, C., Herron, A., Anantha, A., and Howes, T., "LDAP Control Extension for Simple Paged Results Manipulation", RFC 2696, September 1999, http://www.ietf.org/rfc/rfc2696.txt

[RFC2798] Smith, M., "Definition of the inetOrgPerson LDAP Object Class", RFC 2798, April 2000, http://www.ietf.org/rfc/rfc2798.txt

[RFC2891] Howes, T., Wahl, M., and Anantha, A., "LDAP Control Extension for Server Side Sorting of Search Results", RFC 2891, August 2000, http://www.ietf.org/rfc/rfc2891.txt

[RFC4511] Sermersheim, J., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, June 2006, http://www.rfc-editor.org/rfc/rfc4511.txt

[RFC4512] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006, http://www.rfc-editor.org/rfc/rfc4512.txt

[RFC4519] Sciberras, A., Ed., "Lightweight Directory Access Protocol (LDAP): Schema for User Applications", RFC 4519, June 2006, http://www.rfc-editor.org/rfc/rfc4519.txt

[RFC4523] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates", RFC 4523, June 2006, http://www.ietf.org/rfc/rfc4523.txt

[RFC4524] Zeilenga, K., "COSINE LDAP/X.500 Schema", RFC 4524, June 2006, http://www.ietf.org/rfc/rfc4524.txt

[RFC5234] Crocker, D., Ed., and Overell, P., "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008, http://www.rfc-editor.org/rfc/rfc5234.txt

1.2.2 Informative References

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary".

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

1.3 Overview

LDAP, as described in [RFC4511] and [RFC4512], is an Internet protocol that is used for querying and modifying entries in a directory server. LDAP provides a general purpose directory for storing information about objects. The LDAP user schema, as described in [RFC4519], defines a set of attributes for objects contained in a directory server.

This extension defines a set of extensions to LDAP and the LDAP user schema that provides attributes and object types related to the operation of e-mail clients and servers. These attributes and object types include the following:

- New name attributes, organizational attributes, e-mail attributes, and telephone attributes.
- New values of the **objectClass** attribute that identify e-mail groups, remote addresses, and **public folders**.

- A new value of the **supportedControl** attribute that identifies an **AD-type server**.

1.4 Relationship to Other Protocols

This extension defines a set of extensions to LDAP, as described in [RFC4511] and [RFC4512], and the LDAP user schema, as described in [RFC4519].

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

This extension can be used to retrieve information related to the operation of e-mail clients and servers, such as a user's e-mail address or the **mailbox** server that hosts the user's mailbox, from an LDAP server.

1.7 Versioning and Capability Negotiation

This extension does not introduce any versioning constraints beyond those that exist in LDAP, as described in [RFC4511].

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

This extension does not introduce any transport requirements beyond those that exist in LDAP, as specified in [RFC4511].

2.2 Message Syntax

This extension follows the LDAP standard for message syntax, as specified in [RFC4511]. According to the LDAP standard, an attribute list can contain implementation-specific attributes. The attributes specific to this extension are listed in this section.

The following table lists every LDAP attribute for which the client can query. In many cases, more than one LDAP attribute corresponds to a single field in the table below because different server implementations of LDAP use different attribute names to represent similar concepts (fields). In those cases, the attributes listed first in the table take precedence over the attributes listed later. For example, for the **Last Name** field, the **sn** attribute takes precedence over the **surname** attribute. The client only needs to query for one attribute name in each field.

The client SHOULD implement the LDAP user schema, as specified in [RFC4519], the COSINE LDAP/X.500 schema, as specified in [RFC4524], the inetOrgPerson LDAP Object Class, as specified in [RFC2798], and the LDAP X.509 schema, as specified in [RFC4523]. The client SHOULD support the attributes that are listed in the following table.

Field	LDAP attribute
Name attributes	
Display Name	**display-name** (section 2.2.1.1) **displayName** (section 2.2.1.1) **CN** ([RFC4519]) **commonName** ([RFC4519])
Last Name	**sn** ([RFC4519]) **surname** ([RFC4519])
First Name	**givenName** ([RFC4519])
Initials	**Initials** ([RFC4519])
Organizational attributes	
Company Name	**organizationName** ([RFC4519]) **o**<1> ([RFC4519])
Title	**Title** ([RFC4519])
Organizational Unit	**ou** ([RFC4519]) **organizationalUnitName** ([RFC4519]) **department** (section 2.2.2.1)
Office Location	**physicalDeliveryOfficeName** ([RFC4519])
Assistant Name	**secretary** ([RFC4524])

Field	LDAP attribute
Manager	**manager** ([RFC4524])
Reports	**directReports** (section 2.2.2.2) **reports** (section 2.2.2.2)
E-mail attributes	
E-mail Address	**mail** ([RFC4524])
Exchange Distinguished Name	**legacyExchangeDN** (section 2.2.3.2)
Account	**mailNickname** (section 2.2.3.1) **uid** ([RFC4519])
X.400 Address	**TextEncodedORaddress** (section 2.2.3.5)
Exchange Home Server	**msExchHomeServerName** (section 2.2.3.3)
Proxy Addresses	**proxyAddresses** (section 2.2.3.4) **otherMailbox** (section 2.2.3.4)
Physical address attributes	
Address	**postalAddress** ([RFC4519]) **streetAddress** ([RFC4519])
Locality / City	**l** ([RFC4519])
State	**st** ([RFC4519])
Postal Code	**postalCode** ([RFC4519])
Country	**c** ([RFC4519])
Telephone attributes	
Telephone Number	**telephoneNumber** ([RFC4519])
Secondary Phone Number	**Telephone-Office2** (section 2.2.4.2)
Fax Number	**facsimileTelephoneNumber** ([RFC4519])
Assistant Phone Number	**Telephone-Assistant** (section 2.2.4.1)
Home Phone	**homephone** ([RFC4524])
Cell Phone	**mobile** ([RFC4524])
Pager Number	**pager** ([RFC4524])
Notes	**info** ([RFC4524])
Other attributes	
User Certificate	**userCertificate** ([RFC4523])
S/MIME Certificate	**userSMIMECertificate** (section 2.2.5.2)

Field	LDAP attribute
Unused	**user-cert**<2>
Object Class	**objectClass** (section 2.2.5.1)
Role Occupant	**roleOccupant** ([RFC4519])

2.2.1 Extension-Specific Name Attributes

2.2.1.1 Display Name

The **display-name** and **displayName** attributes SHOULD be used as the primary name to be shown to the user when displaying an LDAP entry. If the **display-name** attribute is empty or not user-readable, the client SHOULD construct a **display-name** attribute from other attributes. Applications use implementation-specific logic to construct a **display-name** attribute when needed.<3>

2.2.2 Extension-Specific Organizational Attributes

2.2.2.1 Organizational Unit

The **department** attribute is a multi-valued string attribute that contains the names of any departments or other organizational units to which an object belongs. The syntax of this attribute is the same as the **ou** or **organizationalUnitName** attributes, as specified in [RFC4519].

2.2.2.2 Reports

The **reports** and **directReports** attributes are multi-valued string attributes containing the **distinguished names (DNs) (4)** of any direct reports.

2.2.3 Extension-Specific E-Mail Attributes

2.2.3.1 Account

The **mailNickname** attribute is a multi-valued string attribute that contains login names associated with the object. The syntax of this attribute is the same as the **uid** attribute, as specified in [RFC4519].

2.2.3.2 Exchange Distinguished Name

The **legacyExchangeDN** attribute represents a distinguished name (DN) (4) of the entry. This DN (4) MUST be formatted as specified in [MS-OXOABK] section 2.2.1.1. This value MAY<4> be used as a proxy address for an entry, with the following format.

```
proxyAddressFromExchangeDN ::= "EX:" <Exchange DN>
<Exchange DN> ::= ; The value of the LDAP attribute legacyExchangeDN
```

2.2.3.3 Exchange Home Server

The **msExchHomeServerName** attribute MUST contain the DN (4) of the mailbox server where mail is delivered for that user. For the client, this attribute has the same semantics as the

PidTagAddressBookHomeMessageDatabase property, as specified in [MS-OXOABK] section 2.2.4.67.

2.2.3.4 Proxy Addresses

If multiple e-mail addresses are associated with an entry, they MUST be included in the **proxyAddresses** and **otherMailbox** attributes. These addresses can be used as alternate e-mail addresses to reach the user. Specific e-mail addresses can be retrieved from this value depending on the intended use. The semantics of proxy addresses are not constrained by this extension, and are specific to the protocol that creates the proxy addresses. This extension does not constrain how a client uses proxy addresses. For the client, these proxy addresses have the same semantics as the values of the **PidTagAddressBookProxyAddresses** property, as specified in [MS-OXOABK] section 2.2.3.23.

The format of each e-mail address MUST be as follows.

```
emailString  = <emailType> ":" <emailAddress>
emailType    =  <a string indicating what type of e-mail it is. i.e. SMTP, x500, etc>
emailAddress =  <a string representing the e-mail address>
```

For example, for a **Simple Mail Transfer Protocol (SMTP)** e-mail address of someone@example.com, the resulting value in the **proxyAddresses** or **otherMailbox** attributes would have the following format.

```
SMTP:someone@example.com
```

2.2.3.5 X.400 Address

The **TextEncodedORAddress** attribute is a string attribute that contains a text representation of an X.400 O/R address, as specified in [RFC1274].

2.2.4 Extension-Specific Telephone Attributes

2.2.4.1 Assistant Phone Number

The **Telephone-Assistant** attribute is a string attribute that contains a telephone number for the assistant to the user represented by the directory object.

2.2.4.2 Secondary Phone Number

The **Telephone-Office2** attribute is a string attribute that contains a secondary telephone number for the user represented by the directory object.

2.2.5 Other Extension-Specific Attributes

2.2.5.1 Object Class

The client SHOULD support the following values for the **objectClass** attribute.

Attribute value	Object type
organizationalPerson	This value is specified in [RFC4519].

Attribute value	Object type
groupOfNames group	The groupOfNames value is specified in [RFC4519]. The group value is specific to this extension and is used in the same way as the groupOfNames value.
Remote-Address	This value is specific to this extension and represents a **recipient (2)** that is known to be from a foreign or remote messaging system.
Public-Folder	This value is specific to this extension and represents a place where public discussions take place such as a bulletin board, public folder, or shared folder.

The client SHOULD use the value of the **objectClass** attribute to help distinguish between different types of directory entries when displaying entries to the user. For example, the client can display a different icon or make the item bold to make it easy for a user viewing the object to distinguish its type. If no **objectClass** attribute is returned for an entry, the client MUST treat it as a value of "organizationalPerson".

The value of the **objectClass** attribute is used to determine the value of the **PidTagDisplayType** property, as specified in [MS-OXOABK] section 2.2.3.11. The following **objectClass** attribute values correspond to the following **PidTagDisplayType** property values.

objectClass attribute value	PidTagDisplayType property value
organizationalPerson	DT_MAILUSER
groupOfNames group	DT_DISTLIST
Remote-Address	DT_REMOTE_MAILUSER
Public-Folder	DT_FORUM

2.2.5.2 S/MIME Certificate

The **userSMIMECertificate** attribute contains certificates in the format specified in [RFC2798] or certificates in the format defined for the **PidTagUserX509Certificate** property, as specified in [MS-OXOABK] section 2.2.4.66. If available, this attribute SHOULD be preferred over the **userCertificate** attribute for **S/MIME (Secure/Multipurpose Internet Mail Extensions)** applications.

3 Protocol Details

3.1 Client Details

3.1.1 Abstract Data Model

None.

3.1.2 Timers

None.

3.1.3 Initialization

This extension conforms to the initialization defined by LDAP, as specified in [RFC4511]. In addition, this extension specifies two operations that SHOULD be performed upon connecting to an LDAP server:

- Querying for supported controls. For more details, see section 3.1.3.1.
- Querying for supported capabilities. For more details, see section 3.1.3.2.

3.1.3.1 Querying for Supported Controls

Upon connecting to the LDAP server, the client SHOULD query the server for the **supportedControl** attribute, as specified in [RFC4512]. The **OID (3)** values returned by the server indicate what controls the server supports and makes available to the client. If the client supports browsing the server, it SHOULD recognize the following OID (3) values.

OID value	Supported control
2.16.840.1.113730.3.4.9	Virtual list support ([LDAPEX-SVB])
1.2.840.113556.1.4.319	Paged results support ([RFC2696])
1.2.840.113556.1.4.473	Server sort support ([RFC2891])

3.1.3.2 Querying for Supported Capabilities

Upon connecting to the LDAP server, the client SHOULD query the server for the **supportedCapabilities** custom attribute, as specified in [RFC4511], and MUST recognize the OID (3) value for an AD-type server: "1.2.840.113556.1.4.800".

If the client does not query for this capability, or the server does not return the OID (3) value for an AD-type server, the client MUST treat the server as a non-AD-type server.

When sorting, the protocol client SHOULD use the **displayName** attribute instead of the **CN** attribute on AD-type servers.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

3.1.5.1 Issuing a Search Request

All search requests issued by the client MUST follow the search request definition specified in [RFC4511] section 4.5.1, with the following options specified.

Search request parameter	Value
baseObject	See section 3.1.5.1.1.
Scope	wholeSubtree
derefAliases	derefAlways
typesOnly	FALSE
sizeLimit	Specified by the user.
timeLimit	Specified by the user.
AttributeSelection	CN, commonName, mail, roleOccupant, display-name, displayname, sn, surname, c, organizationName, o, givenName, legacyExchangeDN, objectClass, uid, mailNickname, title, company, physicalDeliveryOfficeName, telephoneNumber
Filter	Depends on the type of search (sections 3.1.5.1.2, 3.1.5.1.3, and 3.1.5.1.4).

3.1.5.1.1 Retrieving a Search Base

A search base is a string representing the DN (4) of the base object entry relative to which a search is to be performed. This value is used as the value of the **baseObject** parameter of a search request, as specified in [RFC4511].

The client can use a user-provided string as the search base. If the user-provided string is an empty string, the client MAY<5> query the server for the **defaultNamingContext** attribute and use the returned value for the search base instead of an empty string. If the user has not specified a search base, the client SHOULD query the server for the **defaultNamingContext** attribute and use the returned value for the search base.

To query the server for the **defaultNamingContext** attribute, the client SHOULD send a search request to the server, as specified in [RFC4511] section 4.5.1, with the following options specified.

Search request parameter	Value
baseObject	Empty string (that is, a zero-length string).
Scope	baseObject
derefAliases	neverDerefAliases
typesOnly	FALSE
sizeLimit	0
TimeLimit	0
Filter	(objectClass=*)

Search request parameter	Value
Attributes	objectClass, defaultNamingContext

3.1.5.1.2 Basic Search Filter

When performing a basic search, the client SHOULD<6> use the following filter as the search filter.

This search filter is specified in **Augmented Backus-Naur Form (ABNF)**, as specified in [RFC5234].

```
basicSearchFilter = "(&(|(mail=" <search-string> "*)(cn=" <search-string>
"*)(sn=" <search-string> "*)(givenName=" <search-string> "*)(displayName="
<search-string> "*)))"search-string =  <a user specified search string>
```

3.1.5.1.3 Advanced Search Filter

The client SHOULD<7> provide a way to search on one or more LDAP attributes. The client SHOULD use strings provided by the user to construct the appropriate LDAP filter.

This search filter is specified in ABNF, as specified in [RFC5234].

```
advancedFilter = "(&(|" *<indvidualAttribute> "))"

individualAttribute = "(" <attributeName> "=" <attributeValue> ")"

attributeName = displayName / display-name / cn / physicalDeliveryOfficeName
/ roomNumber / uid / mailNickname / givenName / sn / telephoneNumber / l
/ title / department / mail

attributeValue = [<containsORbegins>] <userSpecifiedValue> "*"

containsORbegins = "*"; include if searching for a substring, exclude if
                      ; looking for a string beginning with a substring

userSpecifiedValue =  <a user specified value for that field>
```

For each search field requested by the user, the client MUST add all <attributeValue> entries specified in the following table.

Search field	attributeValue
Display Name	displayName (for AD-type servers only) display-name (for AD-type servers only) CN (for non-AD-type servers only)
Office Location	physicalDeliveryOfficeName roomNumber
Account	uid mailNickname
First Name	givenName

Search field	attributeValue
Last Name	sn
Telephone Number	telephoneNumber
Locality / City	l
Title	title
Department	department
E-mail Address	mail

3.1.5.1.4 ANR Search Filter

When the client performs an **ambiguous name resolution (ANR)** search, it SHOULD use the following query.

This search query is specified in ABNF, as specified in [RFC5234].

```
ANRFilter     = "(&(mail=*)(|(mail=" <search-string> "*)(cn=" <search-
string> "*)(sn=" <search-string> "*)(givenName=" <search-string> "*)
(displayName=" <search-string> "*)))" search-string =  <a user specified search string>
```

3.1.5.1.5 Virtual List View Search Filter

If the server indicates support for virtual lists by returning the OID (3) value specified in section 3.1.3.1, clients can generate a Virtual List View, as specified in [LDAPEX-SVB]. Clients SHOULD use the following search filter.

```
VLVFilter = "(&(mail=*)(CN=*))"
```

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 Server Details

3.2.1 Abstract Data Model

None.

3.2.2 Timers

None.

3.2.3 Initialization

This extension conforms to the initialization defined by LDAP, as specified in [RFC4511].

3.2.4 Higher-layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

3.2.5.1 Handling a Query for the supportedControl Attribute

The server MUST respond to a query for the **supportedControl** attribute as specified in [RFC4512]. For each of the following controls it supports, the server MUST return the corresponding OID (3) value.

Supported control	OID value
Virtual list support ([LDAPEX-SVB])	2.16.840.1.113730.3.4.9
Paged results support ([RFC2696])	1.2.840.113556.1.4.319
Server sort support ([RFC2891])	1.2.840.113556.1.4.473

The server SHOULD return other OID (3) values if it provides support for more controls than the ones specified in this extension.

3.2.5.2 Handling a Query for the supportedCapabilities Attribute

The server MUST respond to a query for the **supportedCapabilities** custom attribute as specified in [RFC4511]. If the server supports AD-type server capabilities, as specified in this extension, it MUST return the OID (3) value for an AD-type server: "1.2.840.113556.1.4.800".

The server SHOULD return other OID (3) values if it provides support for more capabilities than the ones specified in this extension.

3.2.5.3 Handling Search Requests

3.2.5.3.1 Handling a Query for the defaultNamingContext Attribute

The server SHOULD respond to a query for the **defaultNamingContext** attribute as specified in section 3.1.5.1.1. If the server returns a value for the **defaultNamingContext** attribute, the server MUST return the DN (4) of the base object.

3.2.5.3.2 Responding to Query Attributes

A server SHOULD support the attributes specified in section 2.2. The client can request more than one attribute representing the same conceptual data. A server is only required to return the value for one of the attributes corresponding to a piece of data requested by the client. For more details about which attributes the client can request, and the order of precedence used when handling return values, see section 2.2

If the server returned the OID (3) value specified in section 3.2.5.2, indicating that it is an AD-type server, it MUST support queries for the **displayname** and **display-name** attributes.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4 Protocol Examples

4.1 Simple Search Scenario

If the client is directed to search for a user named "Robin" in an AD-type server, the following sequence of events occurs:

- The client sends an LDAP Bind request to the server, as described in [RFC4511].

```
BindRequest (0x00):
Version:3
Name:Null
authentication: Authentication type = sasl
```

- The LDAP server receives the request and returns a Bind response to the client, as described in [RFC4511].

```
BindResponse (0x01):
Status: Success
MatchedDN: Null
ErrorMessage: Null
```

- The client sends a search request to the server for the **defaultNamingContext** attribute, as described in section 3.1.5.1.1.

```
SearchRequest (0x03):
BaseObject: Null
Scope: baseObject
Alias: neverDerefAliases
SizeLimit: 0 (no limit)
TimeLimit: 0 (no limit)
TypesOnly: False
Filter: (objectClass=*)
Attributes: (objectClass)(defaultNamingContext)
```

- The LDAP server returns the search base to the client in the **defaultNamingContext** attribute.

```
SearchResultEntry (0x04):
ObjectNames: Null
Attributes Returned:
defaultNamingContext: (DC=company,DC=corp,DC=contoso,DC=com)

SearchResultDone(0x05):
Status: Success
MatchedDN: NULL
ErrorMessage: NULL
```

- The client uses the search base and the simple query described in section 3.1.5.1.2 to send another search request to the server.

```
Search Request (0x03):
BaseObject: (DC=company,DC=corp,DC=contoso,DC=com)
Scope: WholeSubtree
Alias: derefAlways
SizeLimit: 100 entries
TimeLimit: 60 seconds
TypesOnly: False
Filter:(&(|(mail=robin*)(cn=robin*)(sn=robin*)(givenName=robin*)
(displayName=robin*)))Attributes: (cn)(commonName)(mail)(roleOccupant)
(display-name)(displayname)(sn)(surname)(c)(organizationName)(o)(givenName)
(legacyExchangeDN)(objectClass)(uid)(mailNickname)(title)(company)
(physicalDeliveryOfficeName)(telephoneNumber)
```

- The LDAP server returns results that match the query. The trace below represents one result that matched the query.

```
SearchResultsEntry (0x04):
ObjectName: CN=Robin,OU=UsersOU,DC=company,DC=corp,DC=contoso,DC=com
Attributes:
objectClass: ( top ) ( person ) (organizationalPerson ) ( user )
cn: Robin Wood
sn: Wood
title: Dr.
physicalDeliveryOfficeName: 36/2495
telephoneNumber: 1 (425) 555-0534
givenName: Robin
displayName: Robin Wood
company: contoso
mailNickname: robin
legacyExchangeDN: /o=contoso/ou=First Admin Group/cn=Recipents/cn=robin
mail: robin@contoso.com

SearchResultDone(0x05):
Status: Success
MatchedDN: NULL
ErrorMessage: NULL
```

- The client sends an LDAP Unbind request to the server, as described in [RFC4511].

```
UnbindRequest(0x02)
```

- The client uses the attributes returned by the server to display the search results to the user.

5 Security

5.1 Security Considerations for Implementers

There are no security considerations specific to this extension beyond those that exist in LDAP, as specified in [RFC4511].

5.2 Index of Security Parameters

None.

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 released service packs:

- Microsoft® Exchange Server 2003
- Microsoft® Exchange Server 2007
- Microsoft® Exchange Server 2010
- Microsoft® Exchange Server 15 Technical Preview
- Microsoft® Office Outlook® 2003
- Microsoft® Office Outlook® 2007
- Microsoft® Outlook® 2010
- Microsoft® Outlook® 15 Technical Preview

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product 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 2.2: Office Outlook 2003, Office Outlook 2007, and Outlook 2010 query for the **o** attribute, but do not use the value received from the server.

<2> Section 2.2: Office Outlook 2003, Office Outlook 2007, and Outlook 2010 query for the **user-cert** attribute, but do not use the value received from the server.

<3> Section 2.2.1.1: Office Outlook 2003, Office Outlook 2007, and Outlook 2010 consider a **display-name** attribute to be not user-readable if it is exactly the same as one of the **E-Mail Address** attributes. Office Outlook 2003, Office Outlook 2007, and Outlook 2010 construct the **display-name** attribute in the following manner.

```
displayName ::= <common name> / <givenname> " "<surname> / <surname> / <company name> /
<email address> ;
NOTE: Priority is given to non-empty combinations listed first.

common name ::= ; Common Name LDAP attribute
givenname ::= ; First Name LDAP attribute
surname:= ; Last name LDAP attribute
company name ::= ; Organization Name LDAP attribute
email address ::= ; E-Mail Address LDAP attribute
```

<4> Section 2.2.3.2: Office Outlook 2003, Office Outlook 2007, and Outlook 2010 add a proxy address based on the value of the **legacyExchangeDN** attribute to the **proxyAddresses** and **otherMailbox** attributes if it is not present in those attributes on the server.

<5> Section 3.1.5.1.1: If the user-provided string is an empty string, Office Outlook 2003 queries the server for the **defaultNamingContext** attribute and uses the returned value for the search base.

<6> Section 3.1.5.1.2: Office Outlook 2003 does not implement basic bearch.

<7> Section 3.1.5.1.3: Office Outlook 2003 does not support E-Mail (LDAP attribute **mail**) in advanced searches.

7 Change Tracking

This section identifies changes that were made to the [MS-OXLDAP] protocol document between the October 2011 and January 2012 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

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 or functionality.
- An extensive rewrite, addition, or deletion of major portions of content.
- The removal of a document from the documentation set.
- Changes made for template compliance.

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 **Editorial** means that the language and formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical or language changes were introduced. The technical content of the document is identical to the last released version, but minor editorial and formatting changes, as well as updates to the header and footer information, and to the revision summary, may have been made.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.

- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.
- New content added for template compliance.
- Content updated for template compliance.
- Content removed for template compliance.
- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated.**

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

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

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
6 Appendix A: Product Behavior	Added Exchange 15 Technical Preview and Outlook 15 Technical Preview to the list of applicable product versions.	Y	Content updated.

8 Index

A

Abstract data model
  client 13
  server 16
Applicability 7

C

Capability negotiation 7
Change tracking 24
Client
  abstract data model 13
  higher-layer triggered events 13
  initialization 13
  other local events 16
  timer events 16
  timers 13

D

Data model - abstract
  client 13
  server 16

F

Fields - vendor-extensible 7

G

Glossary 5

H

Higher-layer triggered events
  client 13

I

Implementer - security considerations 21
Index of security parameters 21
Informative references 6
Initialization
  client 13
  server 17
Introduction 5

M

Messages
  transport 8

N

Normative references 5

O

Other local events
  client 16
  server 18
Overview (synopsis) 6

P

Parameters - security index 21
Preconditions 7
Prerequisites 7
Product behavior 22

R

References
  informative 6
  normative 5
Relationship to other protocols 7

S

Security
  implementer considerations 21
  parameter index 21
Server
  abstract data model 16
  initialization 17
  other local events 18
  timer events 18
  timers 16
Standards assignments 7

T

Timer events
  client 16
  server 18
Timers
  client 13
  server 16
Tracking changes 24
Transport 8
Triggered events - higher-layer
  client 13

V

Vendor-extensible fields 7
Versioning 7