[MS-OXDSCLI]: Autodiscover Publishing and Lookup Protocol 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.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

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

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

Revision Summary

Date	Revision History	Revision Class	Comments
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		Revised and edited technical content.
12/03/2008	1.03		Revised and edited technical content.
03/04/2009	1.04		Revised and edited technical content.
04/10/2009	2.0		Updated technical content and applicable 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	5.0.0	Major	Updated and revised the technical content.
05/05/2010	5.1.0	Minor	Updated the technical content.

Table of Contents

1 Introduction

This document specifies the Autodiscover Publishing and Lookup protocol, which is used by clients to retrieve **URLs** and settings that are needed to gain access to the Web services that are offered by the server.

1.1 Glossary

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

Active Directory
address book
Autodiscover client
Autodiscover server
display name
distinguished name (DN)
domain
Domain Name System (DNS)
endpoint
enterprise/site/server distinguished name (ESSDN)
fully qualified domain name (FQDN)
GUID
Hypertext Transfer Protocol (HTTP)
Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)
Internet Message Access Protocol (IMAP)
Lightweight Directory Access Protocol (LDAP)
mailbox
offline address book (OAB)
Out of Office (OOF)
Post Office Protocol - Version 3 (POP3)
public folder
remote procedure call (RPC)
rules
Secure Sockets Layer (SSL)
Short Message Service (SMS)
Simple Mail Transfer Protocol (SMTP)
store
Transport Layer Security (TLS)
Uniform Resource Identifier (URI)
Unified Messaging
Uniform Resource Locator (URL)
Web server
XML
XML schema definition (XSD)

The following terms are specific to this document:

Exchange Control Panel (ECP): An Exchange Server feature that provides end users with the ability to manage Exchange options without going through an administrator.

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

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

[MS-OXWOAB] Microsoft Corporation, "Offline Address Book (OAB) Retrieval File Format", April 2008.

[MS-OXWOOF] Microsoft Corporation, "Out of Office (OOF) Web Service Protocol Specification", April 2008.

[RFC2068] Fielding, R., Gettys, J., Mogul, J., et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2068, January 1997, http://www.ietf.org/rfc/rfc2068.txt

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

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

[RFC2518] Goland Y., Whitehead, E., Faizi, A., et al., "HTTP Extensions for Distributed Authoring -- WEBDAV", RFC 2518, February 1999, http://www.ietf.org/rfc/rfc2518.txt

[RFC2616] Fielding, R., Gettys, J., Mogul, J., et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, http://www.ietf.org/rfc/rfc2616.txt

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., et al., "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999, http://www.ietf.org/rfc/rfc2617.txt

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000, http://www.ietf.org/rfc/rfc2818.txt

[RFC2822] Resnick, P., Ed., "Internet Message Format", RFC 2822, April 2001, http://www.ietf.org/rfc/rfc2822.txt

[RFC3986] Berners-Lee, T., Fielding, R., and Masinter, L., "Uniform Resource Identifier (URI): Generic Syntax", RFC 3986, STD 66, January 2005, http://www.ietf.org/rfc/rfc3986.txt

[RFC4120] Neuman, C., Yu, T., Hartman, S., and Raeburn, K., "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005, http://www.ietf.org/rfc/rfc4120.txt

[XML] Bray, T., Paoli, J., Sperberg-McQueen, C., Eds., et al., "Extensible Markup Language (XML) 1.0 (Fifth Edition)", W3C Recommendation, November 2008, http://www.w3.org/TR/REC-xml/

1.2.2 Informative References

[MS-NSPI] Microsoft Corporation, "Name Service Provider Interface (NSPI) Protocol Specification", April 2008, http://go.microsoft.com/fwlink/?LinkID=154742

[MS-OXABREF] Microsoft Corporation, "Address Book Name Service Provider Interface (NSPI) Referral Protocol Specification", April 2008.

[MS-OXCRPC] Microsoft Corporation, "Wire Format Protocol Specification", April 2008.

[MS-OXDISCO] Microsoft Corporation, "Autodiscover HTTP Service Protocol Specification", April 2008.

[MS-OXWAVLS] Microsoft Corporation, "Availability Web Service Protocol Specification", April 2008.

[MS-RPCH] Microsoft Corporation, "Remote Procedure Call over HTTP Protocol Specification", July 2006, http://go.microsoft.com/fwlink/?LinkId=121108

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

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

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL – VERSION 4rev1", RFC 3501, March 2003, http://www.ietf.org/rfc/rfc3501.txt

1.3 Overview

The Autodiscover Publishing and Lookup protocol is a set of methods, headers, and content types that extend the **HTTP**/1.1 protocol. HTTP/1.1 is specified in [RFC2616]. A list of possible **URIs** is first discovered utilizing the [MS-OXDISCO] protocol. The **Autodiscover** service obtains the list of servers of the managed network (**domain**) that are configured with the specified e-mail address. The Autodiscover Publishing and Lookup Protocol enables **Autodiscover clients** to acquire e-mail configuration settings for specific e-mail addresses from the list of **Autodiscover servers** obtained from the [MS-OXDISCO] protocol.

This document specifies the following Autodiscover operations:

- A mechanism for Autodiscover clients to issue queries against Autodiscover servers.
- A mechanism for Autodiscover servers to send client configuration data to Autodiscover clients.
- A mechanism for Autodiscover servers to send referrals to Autodiscover clients.

1.4 Relationship to Other Protocols

The Autodiscover Publishing and Lookup protocol and the Autodiscover HTTP Service protocol [MS-OXDISCO] work together to use the standard HTTP mechanisms defined in [RFC2068] to provide client management over the Internet. The Autodiscover Publishing and Lookup protocol requires the Autodiscover HTTP Service protocol [MS-OXDISCO] to discover the server and to allow Autodiscover clients to find Autodiscover servers that support this protocol. A higher-level protocol, given a server name or URL, uses this protocol to locate the corresponding **FQDN**.

This protocol relies on HTTP 1.1, as specified in [RFC2616]. It relies on **HTTPS**, as specified in [RFC2818], for data protection services.

1.5 Prerequisites/Preconditions

This protocol requires a **Web server** that supports the HTTP POST command.

This protocol also requires that Autodiscover clients have URIs that point to Autodiscover servers. Autodiscover clients can obtain these URIs by using the Autodiscover HTTP Service protocol [MS-OXDISCO].

The Autodiscover Publishing and Lookup protocol assumes that the client has found the Autodiscover server via the Autodiscover HTTP Service protocol, as specified in [MS-OXDISCO].

1.6 Applicability Statement

The Autodiscover Publishing and Lookup protocol is used by a client to discover e-mail configuration settings for a given e-mail address.

1.7 Versioning and Capability Negotiation

Different versions of this protocol can be negotiated by using the <AcceptableResponseSchema> element, which is specified in section 2.2.2.1.

1.8 Vendor-Extensible Fields

Vendors MAY pass additional **XML** elements to Autodiscover clients from the Autodiscover server. To do so, the vendor SHOULD use a separate XML namespace and pass this in the **AcceptableResponseSchema**.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

Messages are transported by using an HTTP POST, as specified in [RFC2518] and [RFC2068].

This protocol SHOULD be used with **SSL**/**TLS**, as specified in [RFC2246]. <1>

2.2 Message Syntax

All **messages** sent between the Autodiscover client and the Autodiscover server are XML messages.

2.2.1 Namespaces

Autodiscover requests are in the "http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/2006" namespace.

Autodiscover responses are in the "http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a" namespace.

2.2.2 Request

The <Request> element contains the request to the Autodiscover service.

The <AcceptableResponseSchema> element and the <EmailAddress> or <LegacyDN> element MUST be child elements of the <Request> element. The expected version is http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a.

The elements specified in the following sections can be child elements of the <Request> element. For an example of the <Request> element, see section 4.

2.2.2.1 AcceptableResponseSchema

The <AcceptableResponseSchema> element identifies the schema for an Autodiscover response.

Clients MUST include this element. The value MUST be the following: http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a.

2.2.2.2 EmailAddress

The <EMailAddress> element identifies the e-mail address of the account for which the configuration information will be retrieved.

This element is an optional element for an Autodiscover request. If it is omitted, the <LegacyDN> MUST be present.

If both the <EmailAddress> and the <LegacyDN> are present, the server MUST use <LegacyDN>.

2.2.2.3 LegacyDN

The <LegacyDN> element identifies a user's **mailbox** by a legacy **distinguished name (DN)**. The <LegacyDN> element is also known as the **enterprise/site/server distinguished name (ESSDN)**, the naming scheme that defines the user.

The <LegacyDN> element is an optional element in the request. If it is omitted, the <EmailAddress> element MUST be present.

If both the <EmailAddress> and the <LegacyDN> elements are present, the server MUST use <LegacyDN>.

2.2.3 Response

The <Response> element contains the response from the Autodiscover server that includes a list of URLs that are used to establish a connection with Web services.

The elements specified in the following sections can be child elements of the <Response> element. For an example that shows the XML schema of the <Response> element and its child elements, see section 4.

2.2.3.1 User

The <User> element and its child elements provide user-specific information. Servers MUST include this element.

The elements specified in the following sections can be child elements of the <User> element.

2.2.3.1.1 DisplayName

The <DisplayName> element represents the user's **display name**.

The server MUST include this element.

2.2.3.1.2 LegacyDN

The <LegacyDN> element identifies a user's mailbox by legacy distinguished name. The <LegacyDN> is also known as the enterprise/site/server distinguished name (ESSDN, the naming scheme that defines the user.

The server MUST include the <LegacyDN> element if EXCH and EXPR protocol sections are returned.

2.2.3.1.3 DeploymentId

The <DeploymentId> element uniquely identifies the server forest in a **GUID** format.

The <DeploymentId> element is returned when the user is within a server forest. The returned value is the GUID identifier of the **Active Directory** forest in which the mailbox user account is contained.

2.2.3.2 Account

The <Account> element specifies account settings for the user or contains error responses.

The elements specified in the following sections can be child elements of the <Account> element.

2.2.3.2.1 AccountType

The <AccountType> element represents the account type. The only allowed <AccountType> value is "email".

2.2.3.2.2 Action

The <Action> element provides information that is used to determine whether another Autodiscover request is required to return the user configuration information.

If the value of <Action> is "settings" (case-insensitive), the Autodiscover server has returned configuration settings in the <Protocol> element.

If the value of <Action> is "redirectAddr" (case-insensitive), the Autodiscover server has returned a <RedirectAddr> element and the Autodiscover client MUST perform another Autodiscover request with the new address.

If the value of <Action> is "redirectUrl" (case-insensitive), the Autodiscover server has returned a <RedirectUrl> element, and the Autodiscover client MUST perform another Autodiscover request with the new URL.

2.2.3.2.3 RedirectAddr

The <RedirectAddr> element specifies the e-mail address that SHOULD be used for a subsequent Autodiscover request. If this element is present, the client SHOULD perform another Autodiscover request by using the e-mail address provided in the <RedirectAddr> element.

The <RedirectAddr> element is returned when the server requires another e-mail address to perform another Autodiscover request. If this element is omitted, the value of the <Action> element is either "settings" or "redirectUrl".

2.2.3.2.4 RedirectUrl

The <RedirectUrl> element contains the URL of the server that SHOULD be used for a subsequent Autodiscover request. If this element is present, the client SHOULD perform another Autodiscover request by using the URL that is provided in the <RedirectUrl> element. <2>

The <RedirectUrl> element is returned when the server requires another URL to perform another Autodiscover request. If this element is omitted, the value of the <Action> element is either settings or redirectAddr.

2.2.3.2.5 Protocol

The <Protocol> element contains the specifications for connecting a client to the server.

The <Protocol> element is returned unless there is a redirection to a <RedirectAddr>. If the server does not return a protocol section, it MUST return a <RedirectAddr>, a <RedirectUrl>, or an error.

If either internal or external access is not available, the <Protocol> element within either the <External> or <Internal> element will be omitted.

The following sections describe elements that can be child elements of <Protocol>.

2.2.3.2.5.1 AD

The <AD> element specifies the Active Directory server used in conjunction with the mailbox. The element contains the FQDN of a **Lightweight Directory Access Protocol (LDAP) server** that the client can connect to for directory information.

2.2.3.2.5.2 ASUrl

The <ASUrl> element specifies the URL of the best **endpoint** instance of Availability Web services for an e-mail enabled user, as specified in [MS-OXWAVLS].

The <ASUrl> element is returned when the server implements a URL for internal or external access.

2.2.3.2.5.3 AuthPackage

The <AuthPackage> element specifies the authentication method that is used when authenticating to the server that contains the user's mailbox. The <AuthPackage> element is used only when the <Type> element has a text value of EXCH or EXPR.

The following are the possible values:

- **basic** — Indicates that the client SHOULD use basic authentication, as specified in [RFC2617].
- **kerb** — Indicates that the client SHOULD use Kerberos authentication, as specified in [RFC4120]
- **kerbntlm** — Indicates that the client SHOULD use Kerberos authentication or NTLM authentication, as specified in [MS-NLMP].
- **Ntlm** — Indicates that the client SHOULD use NTLM authentication.
- **certificate** — Indicates that the client SHOULD use certificate authentication.

The <AuthPackage> element is returned only when there is an external mailbox server authentication method. If the <AuthPackage> is omitted, the client SHOULD use Kerberos or NTLM authentication.

2.2.3.2.5.4 AuthRequired

The <AuthRequired> element specifies whether authentication is required. The following are the possible values:

- on — Authentication is required by the server.
- off — Authentication is not required by the server.

If a value is not specified, the default value is "on".

The <AuthRequired> element is returned only when the <Type> element has a text value of "POP3".

2.2.3.2.5.5 CertPrincipalName

The <CertPrincipalName> element specifies the Secure Sockets Layer (SSL) certificate principal name that is required to connect to the server by using SSL.

If the <CertPrincipalName> element is not specified, the default is set to msstd:SERVER, where SERVER is the value that is specified in the <Server> element. For example, if SERVER is specified as "server.Contoso.com" and <CertPrincipalName> is left blank with SSL turned on, the default value of <CertPrincipalName> would be "msstd:server.Contoso.com".

The <CertPrincipalName> element is returned only when the connection to the server is authenticated with SSL.

2.2.3.2.5.6 DomainName

The <DomainName> element specifies the user's domain. If no value is specified, the default value is the e-mail address in user principal name (UPN) format. For example: <username>@<domain>.

2.2.3.2.5.7 DomainRequired

The <DomainRequired> element contains a text value that indicates whether the domain is required for authentication. The possible values are **on** and **off**. If the value is **on**, the subsequent request must contain the domain of the user's account.

If the domain is not specified in the <LoginName> element, or the <LoginName> element was not specified, the user must specify the domain before authentication will succeed.

2.2.3.2.5.8 EcpUrl

The <EcpUrl> element is the base **Exchange Control Panel (ECP)** URL. The URL contains the following information:

- Protocol – requires "https".
- Host – Host name.
- Path – ECP path within the host server.

The value of the <EcpUrl> element is similar to the following: https://machine.domain.Contoso.com/ecp.

The ECP URLs are formed by joining the <EcpUrl> element with the landing page path for the respective entry points. For example, the full URL for a voice mail link would be <EcpUrl>+<EcpUrl-um> (https://machine.domain.Contoso.com/ecp + ?p=customize/voicemail.aspx&exsvurl=1).<3>

2.2.3.2.5.9 EcpUrl-um

The <EcpUrl-um> element, in conjunction with the <EcpUrl> element, specifies the landing page path for voice mail. The value of the <EcpUrl-um> element is similar to the following: ?p=customize/voicemail.aspx&exsvurl=1.<4>

2.2.3.2.5.10 EcpUrl-aggr

The <EcpUrl-aggr> element, in conjunction with the <EcpUrl> element, specifies the landing page path for e-mail aggregation. The value of the <EcpUrl-aggr> element is similar to the following: ?p=personalsettings/EmailSubscriptions.slab&exsvurl=1. <5>

2.2.3.2.5.11 EcpUrl-sms

The <EcpUrl-sms> element, in conjunction with the <EcpUrl> element, specifies the landing page path for Mobile Notifications/**Short Message Service (SMS)**. The <EcpUrl-sms> element would appear similar to: ?p=sms/textmessaging.slab&exsvurl=1<6>

2.2.3.2.5.12 EcpUrl-mt

The <EcpUrl-mt> element, in conjunction with the <EcpUrl> element, specifies the landing page path for E-Message Tracking. The <EcpUrl-mt> element specified here provides tracking information pertinent to a specific Message. The <EcpUrl-mt> element contains parameters that MUST be substituted by the client as follows:

- <IsOWA> = n.
- <MsgID> = Internet message identifier of the message as specified by the message-id. See [RFC2822].
- <Mbx> = The **SMTP** address of the User's mailbox.
- <Sender> = The SMTP address of the message's sender.

The <EcpUrl-mt> element would appear similar to: PersonalSettings/DeliveryReport.aspx?exsvurl=1&IsOWA=<IsOWA>&MsgID=<MsgID>&Mbx=<Mbx>&Sender=<Sender> <7>

2.2.3.2.5.13 EcpUrl-ret

The <EcpUrl-ret> element, in conjunction with the <EcpUrl> element, specifies the landing page path for retention tags. The value of the <EcpUrl-ret> element is similar to the following: ?p=organize/retentionpolicytags.slab&exsvurl=1.<8>

2.2.3.2.5.14 EwsUrl

The <EwsUrl> element specifies the URL for the Web services virtual directory.

2.2.3.2.5.15 LoginName

The <LoginName> element specifies the user's mail server logon name.

If the domain is not specified in the <LoginName> element, or the <LoginName> element was not specified, the user must specify the domain for authentication to succeed.

2.2.3.2.5.16 MdbDN

The <MdbDN> element represents the legacy distinguished name of the mailbox database.

2.2.3.2.5.17 OABUrl

The <OABUrl> element specifies the **offline address book (OAB)** configuration server URL for a server. See [MS-OXWOAB] for details about the services that are available at this URL.

The <OABUrl> element is returned if there is an internal or external OAB.

2.2.3.2.5.18 OOFUrl

The <OOFUrl> element specifies the URL of the best instance of the Availability service for a mail-enabled user. See [MS-OXWOOF] for details about the services that are available at this URL.

The <OOFUrl> element is returned when the server implements a URL for internal or external access. If the <OOFUrl> element is omitted, the **Out of Office (OOF)** services are not available to the client.

2.2.3.2.5.19 Port

The <Port> element specifies the port that is used to connect to the **store**. See [MS-OXCRPC].

The <Port> element is not returned when the <Server> element contains a URL.

2.2.3.2.5.20 PublicFolderServer

The <PublicFolderServer> element specifies the FQDN for the **public folder** server.

2.2.3.2.5.21 ReferralPort

The <ReferralPort> element specifies the port that is used to get a referral to a directory. For details, see [MS-OXABREF].

2.2.3.2.5.22 Server

The <Server> element specifies the name of the mail server.

The text value identifies the server. For Protocol elements with a Type of EXCH, EXPR, **POP3**, SMTP, or **IMAP**, this value will be either a host name or an IP address.

2.2.3.2.5.23 ServerDN

The <ServerDN> element specifies the distinguished name of the e-mail server. The <ServerDN> element is used only when **Type** is equal to EXCH.

2.2.3.2.5.24 ServerVersion

The <ServerVersion> element represents the version number of the server software. The version number is a 32-bit value expressed in hexadecimal. The <ServerVersion> element is used only when the <Type> element has a value of EXCH or EXPR.

2.2.3.2.5.25 TTL

The <TTL> element specifies the Time to Live (TTL), in hours, during which the settings remain valid. A value of zero indicates that rediscovery is not required.

The <TTL> element is returned when the TTL value is anything other than the default value of 1.

2.2.3.2.5.26 Type

The <Type> element identifies the type of the configured mail account. The following types are defined:

- **EXCH**: The <Protocol> element contains information that the Autodiscover client can use to communicate with the mailbox via **RPC**. For more information, see [MS-OXCRPC]. The <AuthPackage> element, the <ServerVersion> element, or the <ServerDN> element can be used.
- **EXPR**: The <Protocol> element contains information that the Autodiscover client can use to communicate when outside the firewall, including RPC/HTTP connections. For details, see [MS-RPCH]. The <AccountType> element MUST be set to email. The <AuthPackage> element or the <ServerVersion> element can be used.
- **POP3**: The <Protocol> element contains settings that the client can use to communicate with the mail server via the POP3 protocol. For details, see [RFC1939].
- **SMTP**: <Protocol> element contains settings the client can use to send mail via SMTP. For details, see [RFC2821].

- **IMAP**: The <Protocol> element contains settings the client can use to communicate with the mail server via the IMAP protocol. For details, see [RFC3501].
- **DAV**: The <Protocol> element contains settings the client can use to communicate with the mail server via the DAV protocol. For details, see [RFC2518].
- **WEB**: The <Protocol> element contains settings the client can use to connect via a Web browser. The <AccountType> element MUST be set to email.

The server MUST return this element.

2.2.3.2.5.27 SMTPLast

The <SMTPLast> element specifies whether the Simple Mail Transfer Protocol (SMTP) server requires that e-mail be downloaded before it sends e-mail by using the SMTP server. Some ISPs use <SMTPLast> to allow authenticated send.

The possible values are **on** and **off**. If this element is not present, the default value is **off**.

The <SMTPLast> element is used only when Type is equal to SMTP.

2.2.3.2.5.28 SPA

The <SPA> element indicates whether Secure Password Authentication (SPA) is required. If the text value of this element is **on**, SPA is required.

The possible values for this element are **on** and **off**. If this element is not present, the default value is **on**.

2.2.3.2.5.29 SSL

The <SSL> element specifies whether the server requires SSL for logon. The following are the possible values:

- on — SSL is required by the server.
- off — SSL is not required by the server.

If a value is not specified, the default value is "on".

2.2.3.2.5.30 UMUrl

The <UMUrl> element specifies the [RFC3986] URL of the best **instance** of the Unified Messaging Web service for a mail-enabled user.

The <UMUrl> element is returned when the server implements a URL for internal or external access. If the <UMUrl> element is omitted, the Unified Messaging Web service can be unavailable to the client.

2.2.3.2.5.31 UsePOPAuth

The <UsePOPAuth> element indicates whether the authentication information that is provided for a POP3 type of account is also used for SMTP.

The possible values are **on** and **off**.

The <UsePOPAuth> element is used only when Type is equal to SMTP.

2.2.3.2.5.32 Internal

The <Internal> element contains a collection of URLs that a client can connect to when it is inside the firewall.

If the server is configured for internal access, the <Internal> element will contain a <Protocol> element, as specified in section 2.2.3.2.5. The <Protocol> element SHOULD contain an <ASUrl> element (as specified in section 2.2.3.2.5.2) and an <OWAUrl> element (as specified in section 2.2.3.2.5.32.1). The <Protocol> element SHOULD NOT contain any other child elements.

2.2.3.2.5.32.1 OWAUrl

The <OWAUrl> element contained within the <Internal> element describes the [RFC3986] URL and authentication schema that is used to access the server.

The <OWAUrl> can have an **AuthenticationMethod** attribute. This attribute can be one of the following values:

- WindowsIntegrated — Integrated Windows Authentication
- FBA — Forms-based Authentication
- NTLM — NTLM Authentication
- Digest — Digest Authentication
- Basic — Basic Authentication

2.2.3.2.5.33 External

The <External> element contains the collection of URLs that a client can connect to outside the firewall.

The <External> element is returned when the server is configured for an external URL.

If the server is configured for external access, the <External> element will contain a <Protocol> element, as specified in section 2.2.3.2.5. The <Protocol> element SHOULD contain an <ASUrl> element (as specified in section 2.2.3.2.5.2) and an <OWAUrl> element (as specified in section 2.2.3.2.5.32.1). The <Protocol> element SHOULD NOT contain any other child elements.

2.2.3.2.5.34 Encryption

The <Encryption> element is an optional element that is only valid if the <Type> element is set to IMAP, POP3, or SMTP. If the <Encryption> element is present, it overrides the <SSL> element. The following are the possible values of the <Encryption> element:

- None — No encryption is used.
- SSL — SSL encryption is used.
- TLS — TLS encryption is used.
- Auto — The most secure encryption that the client and server support is used.

2.2.3.2.6 AlternativeMailbox

The <AlternativeMailbox> element contains the subelements that represent an additional mailbox that clients can open.

The <AlternativeMailbox> element is returned only when an alternative mailbox is associated with the user. <9>

The elements specified in the following sections can be child elements of the <AlternativeMailbox> element.

2.2.3.2.6.1 Type

The <Type> element identifies the type of the additional mail account.

The only value for this element is archive mailboxes. <10>

2.2.3.2.6.2 DisplayName

The <DisplayName> element represents the additional mailbox user's display name. This string MAY be used to override how a client will display the user's name in the alternative mailbox.<11>

2.2.3.2.6.3 LegacyDN

The <LegacyDN> element identifies the additional mailbox by legacy distinguished name. The <LegacyDN> is also known as the enterprise/site/server distinguished name (ESSDN), the naming scheme that defines the alternative user. <12>

2.2.3.2.6.4 Server

The <Server> element maps to the FQDN of the additional mail server. <13>

2.2.3.2.7 Error

The <Error> element contains an Autodiscover error response, which has two attributes, as listed in the following table.

Attribute	Description
Time	Represents the time when the error response was returned.
Id	Represents a hash of the name of the mail server.

The elements specified in the following sections can be child elements of the <Error> element.

2.2.3.2.7.1 ErrorCode

The <ErrorCode> element contains the error code for an error Autodiscover response.

The following are the current error codes:

- 500 — The e-mail address cannot be found. The Autodiscover server does not know how to provide configuration information for the requested e-mail address.
- 501 — BadAddress. The Autodiscover server knows of the given e-mail address but is unable to provide configuration information because the given e-mail address has no configuration options.

- 601 — The Autodiscover server was unable to provide configuration information of the requested type.
- 602 — Bad Address. The Autodiscover server knows of the given e-mail address but is unable to provide configuration information because of configuration errors.
- 603 — The Autodiscover server threw an internal error.

The list of error codes can expand. Clients MUST accept new error codes.

The <ErrorCode> element is returned when an error occurs.

2.2.3.2.7.2 DebugData

The <DebugData> element contains the debug data for an Autodiscover error response. The contents of this element will depend on the implementation of the Autodiscover server.

The <DebugData> element is returned when an error occurs.

2.2.3.2.7.3 Message

The <Message> element contains the error Message for an error Autodiscover response. The <Message> element SHOULD be in the form of a human-readable error message.

The <Message> element is returned when an error occurs.

3 Protocol Details

The following sections specify details of the Autodiscover Publishing and Lookup Protocol, including abstract data models and message processing **rules**.

3.1 Client Details

3.1.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This **document** does not mandate that implementations adhere to this model as long as their external behavior is consistent with what is described in this document.

It is important for clients to recognize that not all Autodiscover URIs generated by [MS-OXDISCO] or returned in a RedirectAddr reference valid Autodiscover servers. Clients MUST tolerate this and not abandon the Autodiscover operation.

3.1.2 Timers

The available timers:

- HTTP Timeout, as specified in [RFC2068].
- The TTL in the Autodiscover response. Autodiscover clients are asked to respect the TTL. That is, they SHOULD cache the results of an Autodiscover operation and use the cached value if the client needs to Autodiscover that e-mail address again before the TTL expires. The TTL time value is as specified in section 2.2.3.2.5.25.

3.1.3 Initialization

It is assumed the Autodiscover client has an e-mail address for which discover information is needed.

It is assumed the Autodiscover client has a list of URIs that can be Autodiscover server URIs. This list could be generated using the [MS-OXDISCO] protocol. The list could also be preconfigured.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

At a high level, the Autodiscover client SHOULD:

1. Acquire an e-mail address for discovery.
2. Execute the Autodiscover HTTP Service protocol [MS-OXDISCO] with that e-mail address. This will generate a list of URIs that can provide Autodiscover services.
3. Iteratively execute an Autodiscover query against each URI, and do one of the following:
   - If the response to a given query is anything other than a valid Autodiscover Response XML, return to step 3 and issue the query with a different URI.

- If the response contains a <RedirectAddr>, substitute the <RedirectAddr> for the e-mail address and return to step 2.
- If the response contains User, Account, and Protocol Settings, use the settings as needed.
- If the response contains an error, choose the next URI and proceed to step 3.
- If no more URIs are available to Autodiscover against, nothing could be discovered for the given e-mail address.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.1.8 Autodiscover Request

An Autodiscover client requests HTTP POSTs of an Autodiscover XML that contains an e-mail address or <LegacyDN> element. The <LegacyDN> element is also known as the ESSDN.

See section 4.1 for an example of the Autodiscover request.

The <AcceptableResponseSchema> element contains the schema of responses that the client understands. This is shown in section 4.1.

The following are the five categories of responses:

- The URI is not functional. The URI might not be a valid Autodiscover server.
- The HTTP POST returns an HTTP 302 Redirection. In this case, the Autodiscover client SHOULD repost to the redirected server.
- The Autodiscover server returns a <RedirectAddr> element.
- The Autodiscover server returns configuration information.
- The Autodiscover server returns error information.

3.1.8.1 Nonfunctional URIs

[MS-OXDISCO] does not guarantee that the generated URIs are valid Autodiscover server URIs. In addition, network resources can become unavailable for many reasons. When a client reaches a nonfunctional URI, it is best not to abandon the Autodiscover operation. It is recommended to continue the Autodiscover operation.

3.1.8.2 HTTP 302 Redirects

If the server returns a redirection URL via an HTTP 302 Redirect, the client SHOULD repost the request to the redirection URL.

3.1.8.3 Autodiscover Redirect

Autodiscover servers can return a redirection with a redirection address.

See Autodiscover Redirect Example for an example of a redirect address.

3.1.8.4 Autodiscover Configuration Information

See Autodiscover Configuration Example for an example of the Autodiscover Configuration. The Autodiscover Response in the Autodiscover Configuration Example contains a User and an Account with protocol settings.

3.1.8.5 Autodiscover Server Errors

See Autodiscover Server Errors Example for an example of an error returned from an Autodiscover server:

3.2 Server Details

3.2.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with what is described in this document.

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.

3.2.8 Autodiscover Response

An Autodiscover server MUST respond to POSTs to the URL https://<Server>/autodiscover/autodiscover.xml.

The message body of the HTTP POST MUST be an Autodiscover request, as defined in section 2.2.2. See [RFC2068] for details about HTTP POSTs.

If the server does not recognize the e-mail address, it SHOULD respond with a 500 error code. Errors and error codes are defined in section 2.2.3.2.7.

If the server recognizes the e-mail address, but configuration data for that e-mail address could be found if the client issued different Autodiscover request for a more appropriate e-mail address, the server SHOULD respond with a referral (redirection) to that e-mail address. Responses are defined in section 2.2.3. Referral addresses are defined in section 2.2.3.2.3.

If the server is returning configuration information to the client, the server SHOULD construct an Autodiscover response with <User>, <Account>, <Protocol>, and <AlternativeMailbox> sections. These are defined in sections 2.2.3.1, 2.2.3.2, 2.2.3.2.5, and 2.2.3.2.6.

4 Protocol Examples

The following topology is used in this example:

- The **Domain Name System (DNS)** name of the mail server is mail.contoso.com.
- The DNS name of the Web service computer is webservice.contoso.com. It has a valid SSL certificate.
- Autodiscover Web services are available at https://webservice.contoso.com/autodiscover/autodiscover.xml.

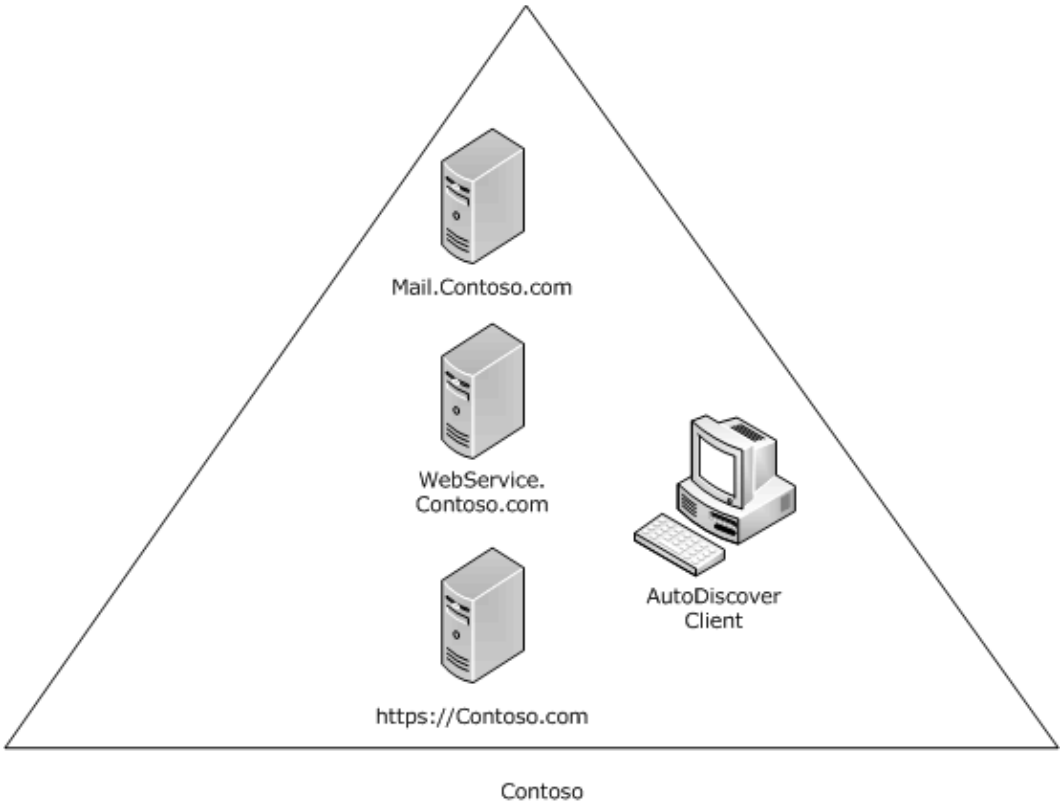

Figure 1: Client and server topology

From executing the Autodiscover HTTP Service protocol [MS-OXDISCO], the client has the following list of possible Autodiscover servers:

- https://contoso.com/autodiscover/autodiscover.xml
- https://webservice.contoso.com/autodiscover/autodiscover.xml

The Autodiscover service is only available on https://webservice.contoso.com/autodiscover/autodiscover.xml, but https://contoso.com/autodiscover/autodiscover.xml is configured to HTTP 302 redirect to https://webservice.contoso.com/autodiscover/autodiscover.xml.

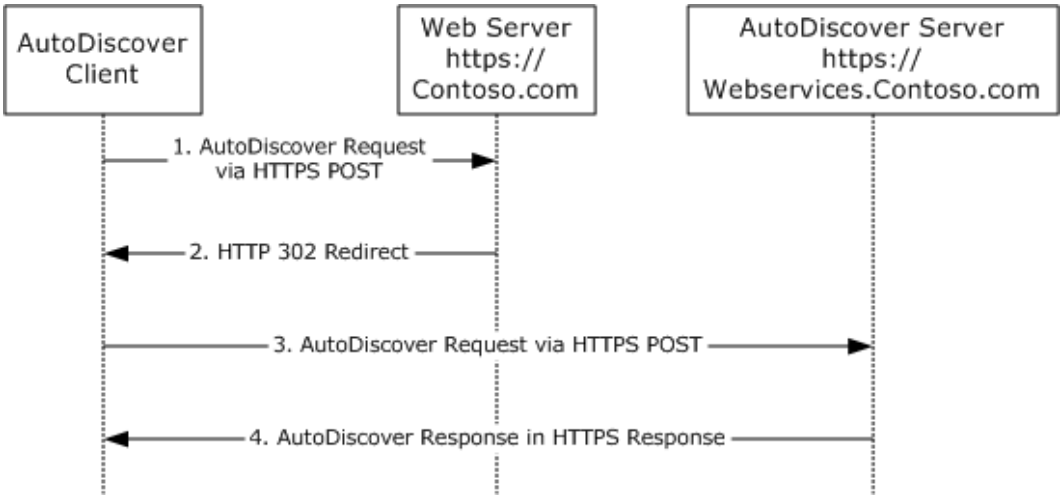

Figure 2: Client and server autodiscovery

Step 1.

The Autodiscover client is configured to use the e-mail address user@contoso.com.

The client constructs the Autodiscover Request XML, as follows.

```
<Autodiscover
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/2006">
   <Request>
     <EMailAddress>user@contoso.com</EMailAddress>
     <AcceptableResponseSchema>
        http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a
      </AcceptableResponseSchema>
   </Request>
</Autodiscover>
```

The client sends the XML via HTTP POST to the following:

https://contoso.com/autodiscover/autodiscover.xml.

Step 2.

The client is returned an HTTP 302 redirection to the following:
https://webservice.contoso.com/autodiscover/autodiscover.xml.

Step 3.

The client then reposts the request to this URL.

Step 4.

The server knows that the mailbox is on mail.contoso.com and that Web services are on https://webservice.contoso.com/autodiscover/autodiscover.xml. The server constructs the following Response XML.<14>

```
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
  <Response
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
    <User>
      <DisplayName>User Display Name</DisplayName>
      <LegacyDN>
         /o=First Organization/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn= User Display Name
        </LegacyDN>
      <DeploymentId>5493afdb-cf6c-4d96-bec3-5709e2d9ad69</DeploymentId>
    </User>
    <Account>
      <AccountType>email</AccountType>
      <Action>settings</Action>
      <Protocol>
        <Type>EXCH</Type>
        <Server>Machine.domain.Contoso.com</Server>
        <ServerDN>
          /o=First Organization/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=machine
        </ServerDN>
        <ServerVersion>738081E2</ServerVersion>
        <MdbDN>
          /o=First Organization/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/
          cn=machine/cn=Microsoft Private MDB
        </MdbDN>
        <AD>machine.domain.Contoso.com</AD>
        <ASUrl>https://machine.domain.Contoso.com/EWS/Exchange.asmx</ASUrl>
        <EwsUrl>https://machine.domain.Contoso.com /EWS/Exchange.asmx</EwsUrl>
        <EcpUrl>https://machine.domain.Contoso.com /ecp</EcpUrl>
        <EcpUrl-um>?p=customize/voicemail.aspx&amp;exsvurl=1</EcpUrl-um>
        <EcpUrl-aggr>?p=personalsettings/EmailSubscriptions.slab&amp;exsvurl=1</EcpUrl-aggr>
        <EcpUrl-sms>?p=sms/textmessaging.slab&amp;exsvurl=1</EcpUrl-sms>
        <EcpUrl-mt>
          PersonalSettings/DeliveryReport.aspx?exsvurl=1&amp;IsOWA=&lt;
        IsOWA&gt;&amp;MsgID=&lt;MsgID&gt;&amp;Mbx=&lt;Mbx&gt;&amp;Sender=&lt;Sender&gt;
        </EcpUrl-mt>
        <EcpUrl-ret>?p=organize/retentionpolicytags.slab&amp;exsvurl=1</EcpUrl-ret>
        <OOFUrl>https://machine.domain.Contoso.com /EWS/Exchange.asmx</OOFUrl>
        <UMUrl>https://machine.domain.Contoso.com /EWS/UM2007Legacy.asmx</UMUrl>
        <OABUrl>http://machine.domain.Contoso.com /OAB/8706ac4e-cde7-4d08-a23f-
9d6be9b58f04/</OABUrl>
      </Protocol>
      <Protocol>
        <Type>WEB</Type>
        <Internal>
          <OWAUrl AuthenticationMethod="Basic, Fba">https://machine.domain.Contoso.com
/owa</OWAUrl>
          <Protocol>
            <Type>EXCH</Type>
            <ASUrl>https://machine.domain.Contoso.com /EWS/Exchange.asmx</ASUrl>
          </Protocol>
        </Internal>
      </Protocol>
      <AlternativeMailbox>
        <Type>Archive</Type>
        <DisplayName>User Archive</DisplayName>
        <LegacyDN>
```

```
          /o=First Organization/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/
          cn=User Display Name/guid=1cfd66a7-23cb-40cb-a735-daddcb98c1b8
        </LegacyDN>
        <Server>machine.domain.Contoso.com </Server>
      </AlternativeMailbox>
    </Account>
  </Response>
</Autodiscover>
```

4.1 Autodiscover Request Example

The following example shows an Autodiscover request.

```
<Autodiscover
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/2006">
   <Request>
     <EMailAddress>user@contoso.com</EMailAddress>
     <AcceptableResponseSchema>
        http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a
      </AcceptableResponseSchema>
   </Request>
 </Autodiscover>
```

The following example shows an Autodiscover response.

```
<AcceptableResponseSchema>
      http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a
</AcceptableResponseSchema>
```

4.2 Autodiscover Redirect Example

The following example shows an Autodiscover redirect.

```
<?xml version="1.0" encoding="utf-8"?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
  <Response
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
    <Account>
      <Action>redirectAddr</Action>
      <RedirectAddr>user@subdomain.contoso.com</RedirectAddr>
    </Account>
  </Response>
</Autodiscover>
```

4.3 Autodiscover Configuration Example

The following example shows an Autodiscover configuration.

```
<?xml version="1.0" encoding="utf-8"?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
```

```
  <Response
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
    <User>
      <DisplayName>User Display Name</DisplayName>
      <LegacyDN>/o=microsoft/ou=Contoso/cn=Recipients/cn=486021</LegacyDN>
      <DeploymentId>30c3a927-42aa-5de8-91e3-8e5b4655ed00</DeploymentId>
    </User>
    <Account>
      <AccountType>email</AccountType>
      <Action>settings</Action>
      <Protocol>
        <Type>EXCH</Type>
        <Server>ExchangeServer.Contoso.com</Server>
        <ServerDN>/o=Contoso/ou=Exchange Administrative Group (GZZHBOHF23SPELT)/
           cn=Configuration/cn=Servers/cn=ExchangeServer</ServerDN>
        <ServerVersion>720180F0</ServerVersion>
        <MdbDN>/o=Contoso/ou=Exchange Administrative Group (GZZHBOHF23SPELT)/
           cn=Configuration/cn=Servers/cn=ExchangeServer/cn=Microsoft Private MDB</MdbDN>
        <PublicFolderServer>PublicFolderServer.Contoso.com</PublicFolderServer>
        <AD>ADServer.Contoso.com</AD>
        <ASUrl>https://mail.Contoso.com/ews/exchange.asmx</ASUrl>
        <EwsUrl>https://mail. Contoso.com/ews/exchange.asmx</EwsUrl>
        <OOFUrl>https://mail. Contoso.com/ews/exchange.asmx</OOFUrl>
        <UMUrl>https://mail. Contoso.com/unifiedmessaging/service.asmx</UMUrl>
        <OABUrl>https://mail. Contoso.com/oab/68b5509d-87f6-4e78-a9ff-74d7d9572787/</OABUrl>
      </Protocol>
      <Protocol>
        <Type>EXPR</Type>
        <Server>RPCHTTPServer.Contoso.com</Server>
        <SSL>On</SSL>
        <AuthPackage>Ntlm</AuthPackage>
        <ASUrl>https://mail.Contoso.com/ews/exchange.asmx</ASUrl>
        <EcpUrl>https://mail.Contoso.com/ecp</EcpUrl>
        <EcpUrl-um>?p=customize/voicemail.aspx&amp;exsvurl=1</EcpUrl-um>
        <EcpUrl-aggr>?p=personalsettings/EmailSubscriptions.slab&amp;exsvurl=1</EcpUrl-aggr>
        <EcpUrl-sms>?p=sms/textmessaging.slab&amp;exsvurl=1</EcpUrl-sms>
        <EcpUrl-mt>PersonalSettings/DeliveryReport.aspx?
          exsvurl=1&amp;IsOWA=&lt;IsOWA&gt;&amp;MsgID=&lt;
          MsgID&gt;&amp;Mbx=&lt;Mbx&gt;&amp;Sender=&lt;Sender&gt;</EcpUrl-mt>
        <EcpUrl-ret>?p=organize/retentionpolicytags.slab&amp;exsvurl=1</EcpUrl-ret>
        <EwsUrl>https://mail.Contoso.com/ews/exchange.asmx</EwsUrl>
        <OOFUrl>https://mail.Contoso.com/ews/exchange.asmx</OOFUrl>
        <UMUrl>https://mail.Contoso.com/unifiedmessaging/service.asmx</UMUrl>
        <OABUrl>https://mail.Contoso.com/oab/58b5509d-87f6-4e78-a9ff-74d7d9572787/</OABUrl>
      </Protocol>
      <Protocol>
        <Type>WEB</Type>
        <External>
          <OWAUrl AuthenticationMethod="Fba">https://mail.Contoso.com/owa</OWAUrl>
          <Protocol>
            <Type>EXPR</Type>
            <ASUrl>https://mail.Contoso.com/ews/exchange.asmx</ASUrl>
          </Protocol>
        </External>
        <Internal>
          <OWAUrl AuthenticationMethod="Ntlm,
WindowsIntegrated">https:/Internal.mail.Contoso.com/owa</OWAUrl>
          <OWAUrl AuthenticationMethod="Basic, Fba">https://mail.Contoso.com/owa</OWAUrl>
          <Protocol>
```

```
            <Type>EXCH</Type>
            <ASUrl>https://mail.Contoso.com/ews/exchange.asmx</ASUrl>
          </Protocol>
        </Internal>
      </Protocol>
    </Account>
  </Response>
</Autodiscover>
```

4.4 Autodiscover Server Errors Example

The following example shows an error that is returned from an Autodiscover server.

```
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
  <Response>
    <Error Time="17:40:40.6157343" Id="3191339394">
      <ErrorCode>500</ErrorCode>
      <Message>The e-mail address cannot be found.</Message>
       <DebugData />
    </Error>
  </Response>
</Autodiscover>
```

5 Security

5.1 Security Considerations for Implementers

Clients SHOULD only perform an Autodiscover request by using this protocol over HTTPS (HTTP with SSL). Not providing SSL will seriously affect the operation of this protocol.

Servers SHOULD NOT answer Autodiscover queries unless the Autodiscover client has authenticated with the Autodiscover server.

5.2 Index of Security Parameters

None.

6 Appendix A: XSDs

6.1 Autodiscover Request XSDs

The following is the Autodiscover Request **XML schema definition (XSD)**. <15>

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema attributeFormDefault="unqualified"
        elementFormDefault="qualified"

targetNamespace="http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/200
6"
        xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="Autodiscover">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Request">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="EMailAddress" type="xs:string" minOccurs="0" />
              <xs:element name="LegacyDN" type="xs:string" minOccurs="0"/>
              <xs:element name="AcceptableResponseSchema" type="xs:string" minOccurs="1"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

6.2 Autodiscover Response XSD

The following is the Autodiscover Response XSD. <16>

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema
xmlns:tns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a"
        attributeFormDefault="unqualified"
        elementFormDefault="qualified"

targetNamespace="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/20
06a"
        xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="Response">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="User">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="DisplayName" type="xs:string" />
              <xs:element name="LegacyDN" type="xs:string" />
              <xs:element name="DeploymentId" type="xs:string" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="Account">
          <xs:complexType>
```

```
            <xs:sequence>
              <xs:element name="AccountType" type="xs:string" />
              <xs:element name="Action" type="xs:string" />
              <xs:element maxOccurs="unbounded" name="Protocol">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element minOccurs="0" name="AD" type="xs:string" />
                    <xs:element minOccurs="0" name="ASUrl" type="xs:string" />
                    <xs:element minOccurs="0" name="AuthPackage" type="xs:string" />
                    <xs:element minOccurs="0" name="AuthRequired" type="xs:string" />
                    <xs:element minOccurs="0" name="CertPrincipalName" type="xs:string" />
                    <xs:element minOccurs="0" name="DomainName" type="xs:string" />
                    <xs:element minOccurs="0" name="DomainRequired" type="xs:string" />
                    <xs:element minOccurs="0" name="EcpUrl" type="xs:string" />
                    <xs:element minOccurs="0" name="EcpUrl-um" type="xs:string" />
                    <xs:element minOccurs="0" name="EcpUrl-aggr" type="xs:string" />
                    <xs:element minOccurs="0" name="EcpUrl-sms" type="xs:string" />
                    <xs:element minOccurs="0" name="EcpUrl-mt" type="xs:string" />
                    <xs:element minOccurs="0" name="EcpUrl-ret" type="xs:string" />
                    <xs:element minOccurs="0" name="Encryption" type="xs:string" />
                    <xs:element minOccurs="0" name="EwsUrl" type="xs:string" />
                    <xs:element minOccurs="0" name="LoginName" type="xs:string" />
                    <xs:element minOccurs="0" name="MdbDN" type="xs:string" />
                    <xs:element minOccurs="0" name="OABUrl" type="xs:string" />
                    <xs:element minOccurs="0" name="OOFUrl" type="xs:string" />
                    <xs:element minOccurs="0" name="Port" type="xs:float" />
                    <xs:element minOccurs="0" name="PublicFolderServer" type="xs:string" />
                    <xs:element minOccurs="0" name="ReferralPort" type="xs:float" />
                    <xs:element minOccurs="0" name="Server" type="xs:string" />
                    <xs:element minOccurs="0" name="ServerDN" type="xs:string" />
                    <xs:element minOccurs="0" name="ServerVersion" type="xs:float" />
                    <xs:element minOccurs="0" name="TTL" type="xs:string" />
                    <xs:element minOccurs="1" name="Type" type="xs:string" />
                    <xs:element minOccurs="0" name="SMTPLast" type="xs:string" />
                    <xs:element minOccurs="0" name="SPA" type="xs:string" />
                    <xs:element minOccurs="0" name="SSL" type="xs:string" />
                    <xs:element minOccurs="0" name="UMUrl" type="xs:string" />
                    <xs:element minOccurs="0" name="UsePOPAuth" type="xs:string" />
                    <xs:element minOccurs="0" name="Internal">
                      <xs:complexType>
                        <xs:sequence>
                          <xs:element name="OWAUrl">
                            <xs:complexType>
                              <xs:simpleContent>
                                <xs:extension base="xs:string">
                                  <xs:attribute name="AuthenticationMethod" type="xs:string"
use="required" />
                                </xs:extension>
                              </xs:simpleContent>
                            </xs:complexType>
                          </xs:element>
                          <xs:element name="Protocol">
                            <xs:complexType>
                              <xs:sequence>
                                <xs:element name="Type" type="xs:string" />
                                <xs:element name="ASUrl" type="xs:string" />
                              </xs:sequence>
                            </xs:complexType>
                          </xs:element>
```

```
                        </xs:sequence>
                      </xs:complexType>
                    </xs:element>
                    <xs:element minOccurs="0" name="External">
                      <xs:complexType>
                        <xs:sequence>
                          <xs:element name="OWAUrl">
                            <xs:complexType>
                              <xs:simpleContent>
                                <xs:extension base="xs:string">
                                  <xs:attribute name="AuthenticationMethod" type="xs:string"
  use="required" />
                                </xs:extension>
                              </xs:simpleContent>
                            </xs:complexType>
                          </xs:element>
                          <xs:element name="Protocol">
                            <xs:complexType>
                              <xs:sequence>
                                <xs:element name="Type" type="xs:string" />
                                <xs:element name="ASUrl" type="xs:string" />
                              </xs:sequence>
                            </xs:complexType>
                          </xs:element>
                        </xs:sequence>
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
              <xs:element name="AlternativeMailbox" minOccurs="0">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="Type" type="xs:string" minOccurs="1" />
                    <xs:element name="DisplayName" type="xs:string" minOccurs="1" />
                    <xs:element name="LegacyDN" type="xs:string" minOccurs="1" />
                    <xs:element name="Server" type="xs:string" minOccurs="1" />
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

6.3 Autodiscover Error Response XSD

The following is the Autodiscover Error Response XSD.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema attributeFormDefault="unqualified"
        elementFormDefault="qualified"

targetNamespace="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006"
```

```
        xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:element name="Autodiscover">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="Response">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="Error">
                  <xs:complexType>
                    <xs:sequence>
                      <xs:element name="ErrorCode" type="xs:unsignedShort" minOccurs="1" />
                      <xs:element name="Message" type="xs:string" minOccurs="1" />
                      <xs:element name="DebugData" minOccurs="1" />
                    </xs:sequence>
                    <xs:attribute name="Time" type="xs:time" use="required" />
                    <xs:attribute name="Id" type="xs:unsignedInt" use="required" />
                  </xs:complexType>
                </xs:element>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:schema>
```

7 Appendix B: Product Behavior

The information in this specification is applicable to the following product versions. References to product versions include released service packs.

- 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 product does not follow the prescription.

<1> Section 2.1: Outlook 2007 and Outlook 2010 will not use Autodiscover servers that do not use SSL.

<2> Section 2.2.3.2.4: The <RedirectUrl> element is not implemented in Exchange 2007 or Exchange 2010.

<3> Section 2.2.3.2.5.8: Exchange 2007 does not support the <EcpUrl> element.

<4> Section 2.2.3.2.5.9: Exchange 2007 does not support the <EcpUrl-um> element.

<5> Section 2.2.3.2.5.10: Exchange 2007 does not support the <EcpUrl-aggr> element.

<6> Section 2.2.3.2.5.11: The <EcpUrl-sms> element is not supported by Exchange 2007.

<7> Section 2.2.3.2.5.12: The EcpUrl-mt element is not supported by Exchange 2007.

<8> Section 2.2.3.2.5.13: Exchange 2007 does not support the <EcpUrl-ret> element.

<9> Section 2.2.3.2.6: Exchange 2007 does not support the *AlternativeMailbox* element.

<10> Section 2.2.3.2.6.1: The <Type> element is not supported by Exchange 2007.

<11> Section 2.2.3.2.6.2: The <DisplayName> element is not supported by Exchange 2007.

<12> Section 2.2.3.2.6.3: The <LegacyDN> element is not supported by Exchange 2007.

<13> Section 2.2.3.2.6.4: The <Server> element is not supported by Exchange 2007.

<14> Section 4: In Exchange 2007, the server constructs the Response XML with the elements modified as specified in section 2.

<15> Section 6.1: The Exchange 2007 server Autodiscover Request XSD is the same, with the elements modified as defined in section 2.

<16> Section 6.2: The Exchange 2007 server Autodiscover Response XSD is the same with the elements modified as defined in section 2.

8 Change Tracking

This section identifies changes made to [MS-OXDSCLI] protocol documentation between February 2010 and May 2010 releases. Changes are classed as major, minor, or editorial.

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.
- A protocol is deprecated.
- The removal of a document from the documentation set.
- Changes made for template compliance.

Minor changes do not affect protocol interoperability or implementation. Examples are updates to fix technical accuracy or ambiguity at the sentence, paragraph, or table level.

Editorial changes apply to grammatical, formatting, and style issues.

No changes means that the document is identical to its last release.

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

- New content added.
- Content update.
- 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 always have the revision type "Editorially updated."

Some important terms used in revision 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.

Changes are listed in the following table. If you need further information, please contact protocol@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
1.1 Glossary	53075 Added "XML schema definition (XSD)" to the list of terms that are defined in [MS-OXGLOS].	N	Content update.
1.3 Overview	Updated the section title.	N	Content updated for template compliance.

9 Index