

[MS-OXDSCLI]: Autodiscover Publishing and Lookup Protocol Specification

Intellectual Property Rights Notice for Protocol Documentation

- **Copyrights.** This protocol 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 protocols, and may distribute portions of it in your implementations of the protocols or your documentation as necessary to properly document the implementation. This permission also applies to any documents that are referenced in the protocol documentation.
- **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 protocols. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, the protocols may be covered by Microsoft's Open Specification Promise (available here: <http://www.microsoft.com/interop/osp/default.mspx>). If you would prefer a written license, or if the protocols are not covered by the OSP, patent licenses are available by contacting protocol@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.

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

Preliminary Documentation. This documentation is preliminary documentation for these protocols. Since the documentation may change between this preliminary version and the final version, 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.

Tools. This protocol documentation is intended for use in conjunction with publicly available standard specifications and networking programming art, and assumes that the reader is either familiar with the aforementioned material or has immediate access to it. A protocol specification does not require the use of Microsoft programming tools or programming environments in order for a Licensee to develop an implementation. Licensees who have access to Microsoft programming tools and environments are free to take advantage of them.

Revision Summary			
Author	Date	Version	Comments
Microsoft Corporation	April 4, 2008	0.1	Initial Availability

Preliminary

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	Protocol Overview (Synopsis).....	7
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.....	8
1.9	Standards Assignments	8
2	Messages.....	8
2.1	Transport.....	8
2.2	Message Syntax.....	8
2.2.1	Namespaces	8
2.2.2	Common Schema	8
3	Protocol Details.....	16
3.1	Client Details	17
3.1.1	Abstract Data Model	17
3.1.2	Timers	17
3.1.3	Initialization.....	17
3.1.4	Higher-Layer Triggered Events.....	17
3.1.5	Message Processing Events and Sequencing Rules	17
3.1.6	Timer Events.....	18
3.1.7	Other Local Events.....	18
3.2	Server Details	22
3.2.1	Abstract Data Model.....	22
3.2.2	Timers.....	22
3.2.3	Initialization.....	22
3.2.4	Higher-Layer Triggered Events.....	22
3.2.5	Message Processing Events and Sequencing Rules	22
3.2.6	NoneTimer Events	22
3.2.7	Other Local Events.....	22
3.2.8	AutoDiscover Request	22
4	Protocol Examples.....	23
5	Security.....	26
5.1	Security Considerations for Implementers.....	26
5.2	Index of Security Parameters.....	26

6	<i>Appendix A: Office/Exchange Behavior</i>	26
7	<i>Appendix B: XSDs</i>	26
7.1	AutoDiscover Request XSDs	26
	<i>Index</i>	28

Preliminary

1 Introduction

The Autodiscover Publishing and Lookup Protocol specified in [MS-OXDISCO] and [MS-OXDSCLI] work together to extend the standard HTTP mechanisms defined in [RFC2068] and provide client management over the Internet. This protocol, [MS-OXDSCLI] requires [MS-OXDISCO] to discover the server and allows AutoDiscover Clients to find AutoDiscover Servers that support this protocol. It also allows AutoDiscover Servers to publish their locations.

1.1 Glossary

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

AutoDiscover Client

AutoDiscover Server

DNS

domain

Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

legacy distinguished name (legacy DN)

Service Connection Point

Secure Sockets Layer (SSL)

The following terms are specific to this document:

Web server: A Web server is a computer running Internet Information Server (IIS) storing web pages that can be retrieved by a client.

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

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

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

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

[RFC2068] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., and T. Berners-Lee, "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", BCP 14, RFC 2119, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>.

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

[RFC2518] Goland, et al, "HTTP Extensions for Distributed Authoring – WEBDAV", RFC 2518, February 1999, <http://www.ietf.org/rfc/rfc2518.txt>.

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

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

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

[XML] Bray, T., Paoli, J., Sperberg-McQueen, C. M., Maler, E., and Yergeau, F., "Extensible Markup Language (XML) 1.0 (Fourth Edition)", <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.

[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. <http://go.microsoft.com/fwlink/?LinkId=113457>cedure Call Over HTTP Protocol Specification", July 2006.

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

[RFC2821] Klensin, J., "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 Protocol Overview (Synopsis)

The Autodiscover Publishing and Lookup Protocol is a set of methods, headers and content types extending the HTTP/1.1 protocol. HTTP/1.1 is specified in [RFC2616]. The Autodiscover Publishing and Lookup Protocol allows AutoDiscover Clients to learn e-mail configuration settings for specific e-mail addresses from AutoDiscover Servers.

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 assumes the client has found the AutoDiscover Server via the Autodiscover HTTP Service protocol

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

1.5 Prerequisites/Preconditions

This specification requires a Web server that supports the POST command.

This specification also requires that AutoDiscover Clients have URIs that point to AutoDiscover servers. AutoDiscover Clients may have obtained these URIs with the Autodiscover HTTP Service protocol.

1.6 Applicability Statement

The Autodiscover Publishing and Lookup Protocol can be 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 using the AcceptableResponseSchema documented in section 2.2.2.1.1.1.1. In Exchange Outlook 2007, the expected version is "http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a".

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 using an HTTP POST as described in [RFC2518] and [RFC2068].

This protocol should be used with SSL/TLS as described in [RFC2246]. Not providing SSL will limit the abilities of client to server communications.

2.2 Message Syntax

All messages sent between the AutoDiscover Client and server are [XML] messages.

2.2.1 Namespaces

For Outlook 2007, AutoDiscover requests must be in the “http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/2006” namespace.

In the response, the AutoDiscover group will be in the “http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006” namespace.

The responses specific to Outlook 2007 will be in the “http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a” namespace.

2.2.2 Common Schema

2.2.2.1 Common Elements

2.2.2.1.1 AutoDiscover

2.2.2.1.1.1 Request

The **Request** element contains the request to the Autodiscover service.

The following elements MAY be child elements of the Request element.

2.2.2.1.1.1.1 AcceptableResponseSchema

The **AcceptableResponseSchema** element identifies the schema for an Autodiscover response.

Clients **MUST** include this element..

2.2.2.1.1.1.2 EmailAddress

The **EmailAddress** element identifies the user's e-mail address.

The EmailAddress element is an alternative element for an Autodiscover request. It is used when a mailbox exists on a computer that is running Exchange.

Clients **MAY** include this element. If omitted, then the LegacyDN **MUST** be present.

If both the EmailAddress and the LegacyDN are present, then the server **MUST** use the LegacyDN.

2.2.2.1.1.1.3 LegacyDN

The **LegacyDN** element identifies a user's mailbox by legacy distinguished name.

The LegacyDN element provides an alternative element for an Autodiscover request.

Clients **MAY** include this element. If omitted then the EmailAddress **MUST** be present.

If both the EmailAddress and the LegacyDN are present, then the server **MUST** use the LegacyDN

2.2.2.1.1.2 Response

The **Response** element contains the response from the Autodiscover service that includes a list of URLs that are used to establish a binding with Web Services.

The following elements may be child elements of response:

2.2.2.1.1.2.1 User

This element group provides user-specific information. Servers **MUST** include this element.

The possible child elements are:

2.2.2.1.1.2.1.1 DisplayName

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

The server **MUST** include this element.

2.2.2.1.1.2.1.2 LegacyDN

The **LegacyDN** element identifies a user's mailbox by legacy distinguished name.

The EmailAddress element is an alternative element for an Autodiscover request. It is used when a mailbox exists on a computer that is running Exchange.

The Server **MUST** include this element if EXCH and EXPR protocol sections are returned.

2.2.2.1.1.2.1.3 *DeploymentId*

The **DeploymentId** element uniquely identifies the Exchange.

The server MAY return this element.

2.2.2.1.1.2.2 *Account*

The **Account** element specifies account settings for the user.

The possible child elements are:

2.2.2.1.1.2.2.1 *AccountType*

The **AccountType** element represents the account type.

If the AccountType is “email” then the setting represent e-mail configuration settings.

2.2.2.1.1.2.2.2 *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 Action is “**settings**” then the AutoDiscover Server has returned configuration settings.

If the Action is “**redirectAddr**” then the AutoDiscover Server has returned a “RedirectAddr” element and the AutoDiscover client MUST perform re-autoDiscover with the new address.

If the Action is “**redirectUrl**” then the AutoDiscover Server has returned a “RedirectUrl” element. The AutoDiscover client MUST perform re-AutoDiscover with the new Url.

The Server MUST return this element.

2.2.2.1.1.2.2.3 *RedirectAddr*

The **RedirectAddr** element specifies the e-mail address that should be used for a subsequent Autodiscover request. If present, the client should AutoDiscover again using the e-mail address provided by RedirectAddr.

The server MAY return this element. If omitted the Action must be of type **settings** or **redirectUrl**.

2.2.2.1.1.2.2.4 *RedirectUrl*

The **RedirectUrl** element contains the URI of the computer that is running Exchange that has the Client Access server role installed that should be used to obtain Autodiscover settings.

The server MAY return this element. If omitted the Action MUST be of type **settings** or **redirectAddr**.

2.2.2.1.1.2.2.5 *Protocol*

The **Protocol** element contains the specifications for connecting a client to the computer that is running Exchange that has the Client Access server role installed.

Servers SHOULD return a protocol section. If they do not return a protocol section, then they MUST return a redirect, or an error.

The following elements MAY be attributes, child elements, and parent elements of this protocol:

2.2.2.1.1.2.2.5.1 ASUrl

The **ASUrl** element specifies the URI of the best endpoint instance of Availability Web Services for a mail-enabled user. See [MS-OXWAVLS].

The server MAY return this element. If omitted then availability services may not be available to Outlook 2007.

2.2.2.1.1.2.2.5.2 AuthPackage

The **AuthPackage** element specifies the authentication scheme that is used when authenticating against the computer that is running Exchange that has the Mailbox server role installed.

The following are the possible values:

- basic
- kerb
- kerbntlm
- Ntlm
- certificate

This list is not exhaustive and may expand in the future.

The server MAY return this element. If omitted then the client should use kerbntlm.

2.2.2.1.1.2.2.5.3 AuthRequired

The **AuthRequired** element specifies whether authentication is required. The possible values are **on** and **off**. If a value is not specified, the default value is **on**.

The server MAY return this element.

2.2.2.1.1.2.2.5.4 CertPrincipalName

The **CertPrincipalName** element specifies the Secure Sockets Layer (SSL) certificate principal name that is required to connect to the Exchange organization 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 Contoso.com and **CertPrincipalName** is left blank with SSL turned on, the default value of **CertPrincipalName** would be msstd:Contoso.com.

The server MAY return this element.

2.2.2.1.1.2.2.5.5 DirectoryPort

The **DirectoryPort** element specifies the port that is used to connect to the directory when the Name Service Provider Interface (NSPI) protocol is used. See [MS-NSPI].

The **DirectoryPort** element is only used when the Type element equals EXCH or EXPR.

Protocol is a parent element of this element.

The server MAY return this element

2.2.2.1.1.2.2.5.6 DomainName

The **DomainName** element specifies the user's domain. If no value is specified, the default authentication is to use the e-mail address as a user principal name (UPN) format. For example: <Username>@<Domain>.

The server MAY return this element.

2.2.2.1.1.2.2.5.7 DomainRequired

The **DomainRequired** element indicates whether the domain is required for authentication. The text value 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.

The server MAY return this element.

2.2.2.1.1.2.2.5.8 Image

The **Image** element contains the path of an image that is used to brand the configuration experience.

The server MAY return this element.

2.2.2.1.1.2.2.5.9 LoginName

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

The server MAY return this element.

2.2.2.1.1.2.2.5.10 MdbDn

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

The server MAY return this element.

2.2.2.1.1.2.2.5.11 OabUrl

The **OABUrl** element specifies the Offline Address Book configuration server URI for an Exchange topology. See [MS-OXWOAB] for details on services available at this URL.

The server MAY return this element. If omitted, the offline address book may not be available to Outlook 2007.

2.2.2.1.1.2.2.5.12 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 on services available at this URL.

The server MAY return this element. If omitted then Out-Of-Office services may not be available to Outlook 2007.

2.2.2.1.1.2.2.5.13 Port

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

The server MAY return this element.

2.2.2.1.1.2.2.5.14 ReferralPort

The **ReferralPort** element specifies the port that is used to get a referral to a directory. See [MS-OXABREF].

The server MAY return this element.

2.2.2.1.1.2.2.5.15 Server

The **Server** element specifies the name of the mail server.

The server SHOULD return this element.

The text value identifies the server. For protocols such as EXCH, EXPR, POP3, SMTP, IMAP, or NNTP, this value will be either a host name or an IP address.

2.2.2.1.1.2.2.5.16 ServerDN

The **ServerDN** element specifies the distinguished name of the computer that is running Exchange Server 2007.

The server MAY return this element.

2.2.2.1.1.2.2.5.17 ServerVersion

The **ServerVersion** element represents the version number of the server software. It is a 32 bit value expressed in hexadecimal.

The server MAY return this element.

2.2.2.1.1.2.2.5.18 ServiceHome

The **ServiceHome** element contains the URL of the home page of the Internet service provider (ISP).

The server MAY return this element.

2.2.2.1.1.2.2.5.19 TTL

The **TTL** element specifies the Time to Live, in hours, during which the settings remain valid. A value of zero indicates that rediscovery is not required. If no value is specified, the default value for this element is 1 hour.

The server **MAY** return this element.

2.2.2.1.1.2.2.5.20 Type

The **Type** element identifies the type of the configured mail account. The following Types are defined:

EXCH: If the type is "EXCH" then the Protocol section contains information the AutoDiscover client can use to communicate with the mailbox via MAPI/RPC. See [MS-OXCRPC].

EXPR: If the type is "EXPR" then the Protocol section contains information the AutoDiscover client can use to communicate when they are outside the firewall, including RPC/HTTP connections. See [MS-RPCH]

POP3: If the Type is "POP3" then the Protocol section contains settings the client can use to communicate with the mail server via the POP3 protocol. See [RFC1939]

SMTP: If the Type is "SMTP" then the Protocol section contains settings the client can use to send mail via SMTP. See [RFC2821].

IMAP: If the Type is "IMAP" then the Protocol section contains settings the client can use to communicate with the mail server via the IMAP protocol. See [RFC3501]

DAV: If the Type is "DAV" then the Protocol section contains settings the client can use to communicate with the mail server via the DAV protocol. See [RFC2518]

WEB: If the Type is "WEB" then the Protocol section contains settings the client can use to connect via a Web browser.

The server **MUST** return this element.

2.2.2.1.1.2.2.5.21 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 server **MAY** return this element. This element is only valid in an SMTP protocol section.

2.2.2.1.1.2.2.5.22 SPA

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

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

The server **MAY** return this element.

2.2.2.1.1.2.2.5.23 SSL

The **SSL** element specifies whether SSL is required for log on.

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

The server MAY return this element.

2.2.2.1.1.2.2.5.24 UMURL

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

The server MAY return this element. If omitted then Unified Messaging services may not be available to Outlook 2007.

2.2.2.1.1.2.2.5.25 UsePOPAuth

The **UsePOPAuth** element indicates whether the authentication information that is provided for a POP3 type of account is also used for Simple Mail Transfer Protocol (SMTP).

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

The server MAY return this element. This element is only valid in a SMTP protocol section.

2.2.2.1.1.2.2.5.26 Internal and External

The **Internal** element contains the collection of Outlook Web Access URLs that a client can connect to when it is inside the firewall. The **External** element contains the collection of Outlook Web Access URLs that a client can connect to outside of the firewall.

The **Internal** and **External** sections may have contained Protocol Group as defined in paragraph 2.2.2.1.1.2.2.5.

The **OWAUrl** element describes the [RFC3986] URL and authentication schema that is used to access a particular computer that is running Exchange Server 2007 that has the Client Access server role installed that hosts Outlook Web Access.

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

- **WindowsIntegrated**: Integrated Windows Authentications
- **FBA**: Forms-based authentication
- **NTLM**: NTLM Authentication
- **Digest**: Digest Authentication
- **Basic**: Basic Authentication

2.2.2.1.1.2.3 Error

The **Error** element contains an Autodiscover error response.

Attribute	Description
Time	Represents the time when the error response was returned.
Id	Represents a hash of the name of the computer that is running Exchange that has the Client Access server role installed.

2.2.2.1.1.2.3.1 *ErrorCode*

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

The current Error codes are:

- 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 MAY expand in the future. Clients MUST accept new error codes.

The server MUST return this element

2.2.2.1.1.2.3.2 *DebugData*

The DebugData element contains the debug data for an Autodiscover error response. The contents will depend on the implementation of the AutoDiscover Server.

This server MAY return this element.

2.2.2.1.1.2.3.3 *Message*

The **Message** element contains the error message for an error Autodiscover response. This SHOULD be a human readable error message.

The server MAY return this element

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 all AutoDiscover URIs generated by [MS-OXDISCO] or returned in a RedirectAddr may not reference valid AutoDiscover Servers. Clients must tolerate this and not abandon the AutoDiscover operation.

3.1.2 Timers

The available timers:

- HTTP Timeout
- 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.

3.1.3 Initialization

It is assumed the AutoDiscover Client has an e-mail address it wants to discover information about.

It is assumed the AutoDiscover Client has a list of URIs that may or may not 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. Acquires an e-mail address it wants to learn about.
2. Executes the [MS-OXDISCO] with that e-mail address. This will generate a list of URIs that may or may not provide AutoDiscover Services.
3. Iteratively execute an AutoDiscoverquery against each URI.
4. If the response to a given query is anything other than an valid AutoDiscover Response XML, then return to step 3 and issue the query with a different URI.

5. If the Response Group contains a RedirectAddr, then substitute the redirectAddr for the e-mail address and return to step 1.
6. If the Response Group contains a RedirectURL, then issue an AutoDiscover query against the RedirectURL and proceed to step 3.
7. If the Response Group contains User, Account and Protocol Settings, then use the settings as needed.
8. If the Response Group contains an error, then choose the next URI and proceed to step 3.
9. If no more URIs are available to AutoDiscover against, then nothing could be discovered for the given e-mail address.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.1.7.1 AutoDiscoverRequest

AutoDiscover Client requests HTTP Posts of an AutoDiscover XML that contains an e-mail address or legacyDN.

example:

```
<Autodiscover
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/requests
chema/2006">
  <Request>
    <EmailAddress>user@contoso.com</EmailAddress>

    <AcceptableResponseSchema>http://schemas.microsoft.com/exchange/autodiscov
er/outlook/responseschema/2006a</AcceptableResponseSchema>
  </Request>
</Autodiscover>
```

Or

```
<Autodiscover
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/requests
chema/2006">
  <Request>

    <LegacyDN>/o=microsoft/ou=Contoso/cn=Recipients/cn=486021</LegacyDN>

    <AcceptableResponseSchema>http://schemas.microsoft.com/exchange/autodiscov
er/outlook/responseschema/2006a</AcceptableResponseSchema>
  </Request>
</Autodiscover>
```

The AcceptableResponseSchema is the schema of responses that the client understands. For Outlook 2007 this is:

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

The following are the five categories of responses.

- The URI is not functional. The URI may 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 or an Redirect URI
- The AutoDiscover Server returns configuration Information.
- The AutoDiscover Server returns error information.

3.1.7.1.1 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 must not abandon the AutoDiscover operation. It must continue.

3.1.7.1.2 HTTP 302 Redirects.

If the POST returns a redirection URL via an HTTP 302 Redirect, then the client should repost the request to the redirection URL.

3.1.7.1.3 AutoDiscover Redirects

AutoDiscover Servers can return two forms of redirection. A Redirection Address or a Redirection URL.

An example of a redirect address is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<Autodiscover
xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006a">
  <Response
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
    <Account>
      <Action>redirectAddr</Action>
      <RedirectAddr>user@subdomain.contoso.com</RedirectAddr>
    </Account>
  </Response>
</Autodiscover>
```

An example of a redirect URL is as follows:

```
<?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/response
schema/2006a">
    <Account>
      <Action>redirectUrl</Action>

<RedirectUrl>https://subdomain.contoso.com/AutoDiscover/AutoDiscover.xml</
RedirectUrl>
    </Account>
  </Response>
</Autodiscover>
```

3.1.7.1.4 AutoDiscover Configuration Information

What follows is an example of AutoDiscover Configuration. The AutoDiscover Response contains a User and an Account with protocol settings.

```
<?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/response
schema/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=Microso
ft 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>
        <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>

```

3.1.7.1.5 *AutoDiscover Server Errors.*

Below is an example of an error returned from an AutoDiscover Server:

```

<Autodiscover
xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2
006">
    <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>

```

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

3.2.6 NoneTimer Events

None.

3.2.7 Other Local Events

None.

3.2.8 AutoDiscover Request.

An AutoDiscover Server should respond to POSTS to the URL.

<https://<Server>/autoadiscovers/autodiscovers.xml>

The message body of the HTTP Post should be an XML AutoDiscover Request as defined in 2.2.2.1.1.1. See [RFC2068] for details on HTTP Posts.

If the Server does not recognize the e-mail address, it should respond with a 501 error code. Errors and Error Codes are defined in section 2.2.2.1.1.2.3.

If the Server recognizes the e-mail address, but knows that configuration data for that e-mail address could be found if the client issued different AutoDiscover Request for a more appropriate e-mail address, then the server should respond with a referral to that e-mail address. Responses are defined in 2.2.2.1.1.2. Referral Addresses are defined in 2.2.2.1.1.2.2.2 and 2.2.2.1.1.2.2.3

If the server wants to redirect the client to another server, it should return a redirect URL response. Redirect URL responses are defined in 2.2.2.1.1.2.2.4.

If the server wants to return configuration information to the client, then the server should construct an AutoDiscover Reponse with <User>, <Account> and <Protocol> sections. These are defined in 2.2.2.1.1.2.1, 2.2.2.1.1.2.2, and 2.2.2.1.1.2.2.5.

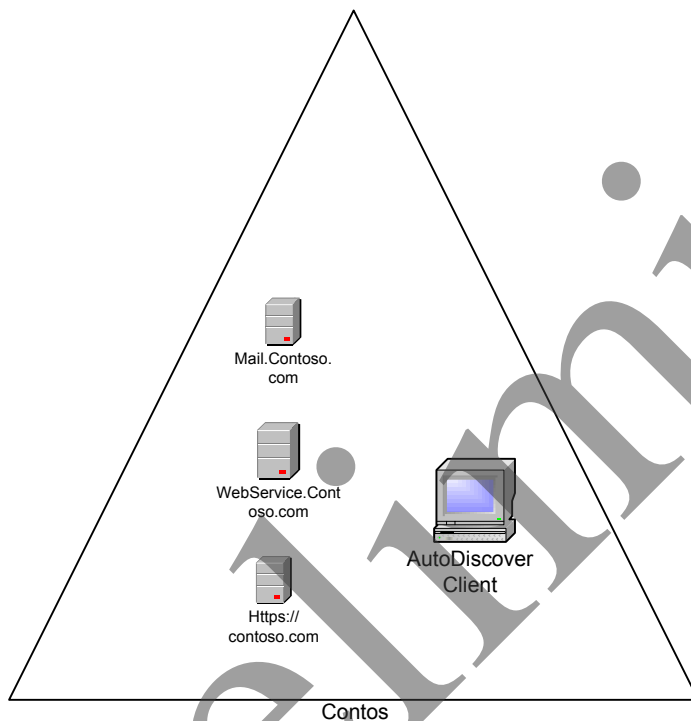
4 Protocol Examples

Assume the following topology:

The 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>



From executing [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>

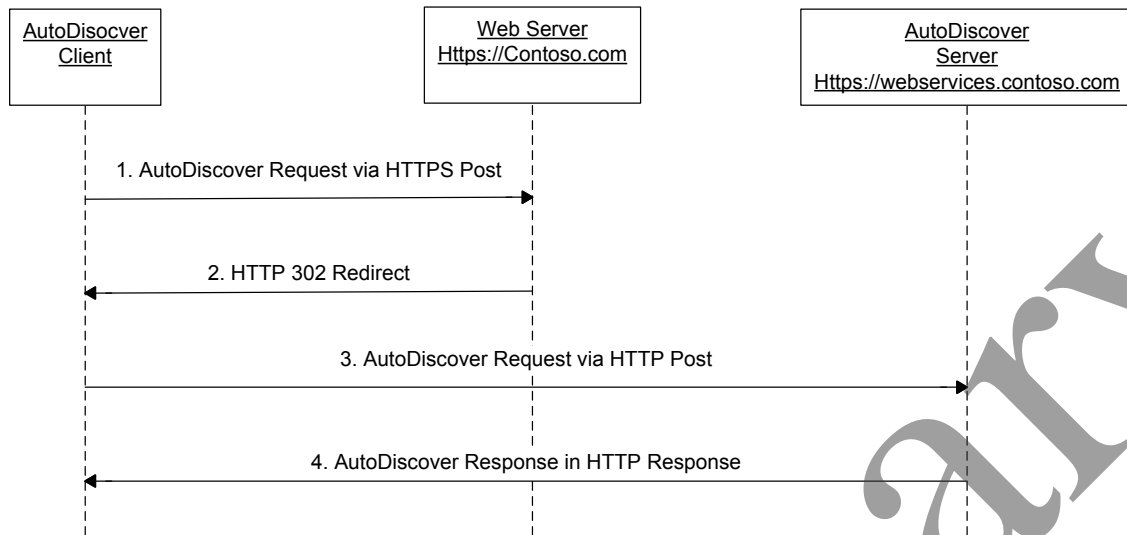


Figure 1: Client and Server AutoDiscovery

Step 1.

The AutoDiscover client is configured to use the e-mail address User@Contoso.com.

The client constructs the AutoDiscover Request XML:

```

<Autodiscover
  xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/requests
  chema/2006">
  <Request>
    <EmailAddress>user@contoso.com</EmailAddress>
    <AcceptableResponseSchema>http://schemas.microsoft.com/exchange/autod
  iscover/outlook/responseschema/2006a</AcceptableResponseSchema>
  </Request>
</Autodiscover>
  
```

and HTTP Posts it to:

<https://Contoso.com/AutoDiscover/AutoDiscover.xml>

Step 2.

The client is returned a HTTP 302 redirection to:

<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>. It constructs and returns the following Response XML.

```
<?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/response
    schema/2006a">
    <User>
      <DisplayName>User Display Name</DisplayName>

<LegacyDN>/o=Contoso/ou=Contoso/cn=Recipients/cn=User</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=Microso
        ft Private MDB</MdbDN>
        <PublicFolderServer>Mail.Contoso.com</PublicFolderServer>
        <AD>MailLdap.Contoso.com</AD>

<ASUrl>https://WebService.Contoso.com/ews/exchange.asmx</ASUrl>

<EwsUrl>https://WebService.Contoso.com/ews/exchange.asmx</EwsUrl>

<OOFUrl>https://WebService.Contoso.com/ews/exchange.asmx</OOFUrl>

<UMUrl>https://WebService.Contoso.com/unifiedmessaging/service.asmx</UMUrl
>
      <OABUrl>https://WebService.Contoso.com/oab/68b5509d-87f6-
      4e78-a9ff-74d7d9572787</OABUrl>
    </Protocol>
  </Account>
</Response>
</Autodiscover>
```

5 Security

5.1 Security Considerations for Implementers

Office/Exchange Behavior: Outlook will not perform an auto discovery using this protocol unless it is over HTTPS (HTTP with SSL)

Office/Exchange Behavior: Exchange will not answer AutoDiscover queries unless the AutoDiscover client has authenticated with the AutoDiscover Server.

5.2 Index of Security Parameters

None.

6 Appendix A: Office/Exchange Behavior

The information in this specification is applicable to the following versions of Office/Exchange:

- Office 2003 with Service Pack 3 applied
- Exchange 2003 with Service Pack 2 applied
- Office 2007 with Service Pack 1 applied
- Exchange 2007 with Service Pack 1 applied

Exceptions, if any, are noted below. Unless otherwise specified, any statement of optional behavior in this specification prescribed using the terms SHOULD or SHOULD NOT implies Office/Exchange behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies Office/Exchange does not follow the prescription.

By default, Exchange Server 2007 only provides this protocol via HTTP with SSL (HTTPS). Outlook 2007 and Outlook2007 with Service Pack 1 applied will only use this protocol via HTTPS. Not providing SSL will seriously affect the operation of this protocol.

7 Appendix B: XSDs

7.1 AutoDiscover Request XSDs

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="requestschema2006"
targetNamespace="http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/2006" elementFormDefault="qualified"
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/2006"
```

```
xmlns:mstns="http://schemas.microsoft.com/exchange/autodiscover/outlook/re  
questschema/2006" xmlns:xs="http://www.w3.org/2001/XMLSchema">
```

```
  <xs:element name="Autodiscover">  
    <xs:complexType>  
      <xs:sequence>  
        <xs:element name="Request" type="RequestType" />  
      </xs:sequence>  
    </xs:complexType>  
  </xs:element>  
  
  <xs:complexType name="RequestType">  
    <xs:sequence>  
      <xs:sequence>  
        <xs:element name="EmailAddress" type="xs:string"  
minOccurs="0" maxOccurs="1"/>  
        <xs:element name="LegacyDN" type="xs:string"  
minOccurs="0" maxOccurs="1" />  
        <xs:element name="AcceptableResponseSchema"  
type="xs:string" minOccurs="1" maxOccurs="1"/>  
      </xs:sequence>  
    </xs:sequence>  
  </xs:complexType>  
  
</xs:schema>  
I
```

Index

Appendix A

Office/Exchange Behavior, 26

Appendix B

XSDs, 26

AutoDiscover request XSDs, 26

Introduction, 5

Applicability Statement, 7

Glossary, 5

Prerequisites/Preconditions, 7

Protocol overview (synopsis), 7

References, 5

Relationship to other protocols, 7

Standards assignments, 8

Vendor-extensible fields, 8

Versioning and capability negotiation, 7

Messages, 8

Message syntax, 8

Transport, 8

Protocol details, 16

Client details, 17

Server details, 22

Protocol examples, 23

References

Informative references, 6

Normative references, 5

Security, 26

Index of security parameters, 26

Security considerations for implementers, 26