[MS-OXDISCO]: Autodiscover HTTP Service 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

Table of Contents

1 Introduction

The Autodiscover HTTP Service Protocol extends DNS and directory services to make available the location and settings of mail servers which provide clients with functionality as described in the Autodiscover Publishing and Lookup Protocol.

1.1 Glossary

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

Active Directory (AD)
AutoDiscover Client
AutoDiscover Server
distinguished name (DN)
GUID
Lightweight Directory Access Protocol (LDAP)
LDAP server
Secure Sockets Layer (SSL)
URI
XML

The following terms are specific to this document:

AutoDiscover Directory Service Map GUID: A globally unique identifier designated GUID 67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68, which identifies Service Connection Points which identify other directory service forests that possibly contain AutoDiscover Server information.

AutoDiscover URI Map GUID: A globally unique identifier designated GUID 77378F46-2C66-4aa9-A6A6-3E7A48B19596, which identifies Service Connection Points which identify AutoDiscover Server URIs.

common name: A string attribute of a certificate that is one component of a distinguished name (DN). In Microsoft Enterprise uses, a CN must be unique within the forest where it is defined and any forests that share trust with the defining forest. The Web site or e-mail address of the certificate owner is often used as a common name. Client applications often refer to a certificate authority (CA) by the CN of its signing certificate.

Domain Name System (DNS): A hierarchical, distributed database that contains mappings of domain names to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database.

Hypertext Transfer Protocol (HTTP): An application-level protocol for distributed, collaborative, hypermedia information systems (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS): HTTPS is an extension of HTTP that securely encrypts and decrypts Web page requests.

LDIF: LDAP Data Interchange Format. See [RFC2849]

Port: A TCP IP Port. See "Names, Addresses, Ports, and Routes" [RFC814]

Service Binding Information: The URI needed to bind to a service.

Service Connection Point: An object made available via a directory service that clients can use to discover AutoDiscover Servers. See [MS-ADTS].

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

[RFC1034] Mockapetris, P., "Domain Names–Concepts and Facilities", RFC 1034, November 1987, http://www.ietf.org/rfc/rfc1034.txt.

[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.

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

[RFC2251] Wahl, M., Howes, T., and Kille, S., "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997, http://www.ietf.org/rfc/rfc2251.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.

[RFC2782] Gulbrandsen, A., P. Vixie, A., and Esibov, L., "DNS RR for specifying the location of services (DNS SRV)", RFC 2782, http://www.ietf.org/rfc/rfc2782.txt.

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

[RFC2849] Good, G., "LDAP Data Interchange Format (LDIF)", RFC 2849, June 2000, http://www.ietf.org/rfc/rfc2849.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.

[RFC4516] Howes, T., et al, "Lightweight Directory Access Protocol (LDAP) Uniform Resource Locator", RFC 4516, June 2006, http://www.ietf.org/rfc/rfc4516.txt.

1.2.2 Informative References

[MS-ADTS] Microsoft Corporation, "Active Directory Technical Specification", July 2006, http://go.microsoft.com/fwlink/?LinkId=112149.

[MS-OXDSCLI] Microsoft Corporation, "Autodiscover Publishing and Lookup Protocol Specification", April 2008.

[MSDN-ASP] Microsoft Corporation, "Active Server Pages", http://go.microsoft.com/fwlink/?LinkId=112503.

[RFC1034] Mockapetris, P., "Domain Names–Concepts and Facilities", RFC 1034, November 1987, http://www.ietf.org/rfc/rfc1034.txt.

[RFC1035] Mockapetris, P., "Domain Names—Implementation and Specification", RFC 1035, November 1987, http://www.ietf.org/rfc/rfc1035.txt.

[RFC2510] Adams, C., "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999, http://www.ietf.org/rfc/rfc2510.txt.

1.3 Protocol Overview (Synopsis)

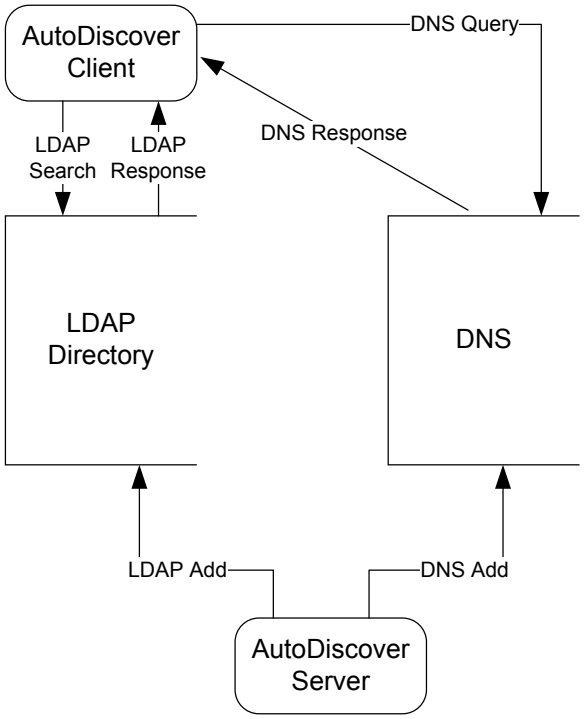
The AutoDiscover HTTP Service Protocol allows a managed network (domain) to expose **AutoDiscover Servers** to clients configured with an e-mail address.

URIs to AutoDiscover Server locations can be published via the following:

- **Service Connection Points** which can be queried via **Lightweight Directory Access Protocol (LDAP)**
- Direct DNS configuration
- DNS SRV record configuration
- HTTPS 302 redirection

1.4 Relationship to Other Protocols

This specification requires an AutoDiscover Server and an **AutoDiscover Client** that implement the Autodiscover Publishing and Lookup Protocol [MS-OXDSCLI]. This protocol relies on HTTPS as defined in [RFC2818] for data protection services and it relies on [RFC1034] for DNS services. It also relies on [MS-ADTS] and [RFC1823] for the Service Connection Point and **LDAP**.



1.5 Prerequisites/Preconditions

The AutoDiscover Client SHOULD be configured with an LDAP Directory and base DN that is well known to the AutoDiscover Server Administrator.
The AutoDiscover Server SHOULD be configured with SSL.

1.6 Applicability Statement

This protocol is applicable in scenarios where an e-mail client wants to discover e-mail server settings and e-mail servers that want to publish their locations and settings.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

For the purposes of this protocol an AutoDiscover Client and an AutoDiscover Server do not communicate directly. Instead the AutoDiscover Client communicates with common well known data sources that the AutoDiscover Server Administrator has preconfigured.

The following Transports and Data Sources are used:

1. LDAP and LDAP Directories. See [RFC1823].
2. The DNS and DNS SRV Records. See [RFC1034] and [RFC2792].
3. HTTP and HTTP 302 redirection. See [RFC2616].

2.2 Message Syntax

2.2.1 SCP Objects

2.2.1.1 The LDIF form of Service Connection Points

From LDIF as referenced in [RFC2849], a Service Connection Point can be expressed as the following:
Dn: <distingushedName>
ObjectClass: serviceConnectionPoint
Keyword: <KeywordValue>
[Keyword: <KeywordValue>]
ServiceBindingInformation:<serviceBindingInformationValue>

That is, a Service Connection Point has a <distinguishedName> , has one or more <KeywordValues> and one <serviceBindingInformationValue>.

2.2.1.2 Searches for SCP Objects

The following LDAP elements and operations are used to search for an SCP object.

- <host> is a server running LDAP This value SHOULD be well known to the AutoDiscover Client and the AutoDiscover Server Administrator.
- <port> is the port of the of the LDAP service on <host>. This value is commonly 389. This value should be well known to the AutoDiscover Client and AutoDiscover Server Administrator.
- <DN> is the DistinguishedName to base the search on. This value should be well known to the AutoDiscover Server and the AutoDiscover Client.
- <SCOPE> is the Search Scope. For AutoDiscover clients this MUST be LDAP_SCOPE_SUBTREE. This is a constant defined in [RFC1823].
- The list of attributes to query for. For the purposes of this protocol, the list MUST contain “ServiceBindingInformation”, and “Keywords”.

- An LDAP filter, as specified in [RFC1558]. For the purposes of this protocol, <filter> is "(&(objectclass=`serviceConnectionPoint)(|(keywords=67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68)( keywords=77378F46-2C66-4aa9-A6A6-3E7A48B19596)))`"

The search MAY be performed using the LDAP API [RFC1823].

2.2.1.3 Creating SCP Objects

Service Connection Points can be created in an LDAP directory. To do so, the administrator needs the following data elements…

- A <host>.running an LDAP server. This value should be well known to the AutoDiscover Client and AutoDiscover Server Administrator.
- The <port> of the LDAP service on <host>. This value is typically 389. This value should be well known to the AutoDiscover Client and AutoDiscover Server Administrator.
- A DN (DistinguishedName) to base the search. This value should be well known to the AutoDiscover Server Administrator and the AutoDiscover Client.
- The list of attributes to write for. For the purposes of this protocol, the list MUST contain "ServiceBindingInformation", and "Keywords"
- The list of values for the attributes "ServiceBindingInformation" and the "Keywords" These values are discussed in Section 3.
- The <objectclass> to create. For the purposes of this protocol, the object class MUST be "ServiceConnectionPoint"

2.2.2 DNS SRV Queries

To query for AutoDiscover Servers, the AutoDiscover Client should use the following data elements as per the Usage Rules in [RFC2782]:

_service is "_AutoDiscover"
_protocol is "_tcp"
The target is supplied by the AutoDiscover Client.

The query produces an ordered list of hosts.

2.2.3 HTTP 302 Redirection

The following section uses Augmented Backus-Naur Form notation. See [RFC5234].

The AutoDiscover Client MAY request an HTTP GET of the Request-Uri
<RequestUri> = HTTP COLON SLASH SLASH AUTODISCOVERDOT <target> AUTODISCOVERSUFFIX

HTTP = "http"
COLON = ":"
SLASH = %2f ; forward slash or "/"

AUTODISCOVERDOT = “AutoDiscover.”
AUTODISCOVERSUFFIX = SLASH “AutoDiscover” SLASH “AutoDiscover.xml”
<target> = targetDomain ; The e-mail domain that the AutoDiscover Client wishes to query.

The above strings are not case sensitive.

<Request-URI> can be processed as per [RFC2616], Section 9.3. If the response is a 302 Redirection (See section 10.3.3 of [RFC2616], the AutoDiscover Client uses the value of the Redirection Url.

2.2.4 E-mail Addresses

All e-mail addresses are assumed to be in the format defined in [RFC2822] Section 3.4.1 That is, they are <local-part> “@” <domain>.

2.2.5 The List of Possible AutoDiscover Server URIs

The result of this protocol is a list of Possible AutoDiscover Server URIs. URIs are defined in [RFC3986].

3 Protocol Details

This protocol specifies a way for AutoDiscover Clients to find AutoDiscover Servers. The protocol starts with an e-mail address of the form <mailbox>@<domain> and expands it to a list of URIs any of which can be AutoDiscover Servers.

3.1 Client Details

3.1.1 Abstract Data Model

The MS-OXDISCO algorithm takes an e-mail address of the form <local-part> @ <Domain> and expands it into a list of URIs as defined in [RFC2396]. To create this list, the AutoDiscover Client needs to do one of the following:

- Query a well known LDAP server for Service Connection Points.
- Perform text manipulations on the domain of the email address.
- Search the DNS for _AutoDiscover SRV records and.
- Perform an HTTP GET to determine if there are redirects to other AutoDiscover Servers.

3.1.2 Timers

None.

3.1.3 Initialization

The client uses an e-mail address of the form <local-part> "@" <Domain>

3.1.4 Abstract Data Types

The AutoDiscover Client maintains a list of possible AutoDiscover Server URIs.

3.1.5 Query a Well Known LDAP Server for Service Connection Points

AutoDiscover Server locations MAY be published in LDAP directories via Service Connection Point objects

To discover these servers, AutoDiscover Clients execute a client search as outlined in section 2.2.1.2.

For each of the entries returned, if the ServiceBindingInformation attribute is an LDAP URI (a text string of the form "LDAP://"<host>[:<port>]) and the KeywordsAttribute contains a string of the form "Domain="<domain>), then the client repeats the search as outlined in section 2.2.1.2 with the new <host> and <port> values.

If the ServiceBindingInformation attribute is an LDAP URI (a text string of the form "LDAP://"<host>[:<port>]), but the KeywordsAttribute does not contain a string of the form "Domain="<domain>, then the client repeats the search as outlined in section 2.2.1.2 with the new <host> and <port> values after all other entries have been evaluated.

If the ServiceBindingInformationAttribute is an "HTTP://" URI then the client has found a URI that is possibly an AutoDiscover Server and the client adds this to the list of possible AutoDiscover Servers.

If the **AutoDiscover Directory Service Map GUID** is found in the Keywords, then the serviceBindingInformation is an LDAP URI. If the **AutoDiscover URI Map GUID** is found in the Keywords, then the serviceBindingInformation is an HTTP URI.

3.1.6 Locations Found Directly From the E-mail Domain.

The following two URIs MUST be added to the list of possible AutoDiscover Server URIs

"HTTPS://" <Domain>"AutoDiscover/AutoDiscover.xml"
"HTTPS://" "AutoDiscover."<Domain>"AutoDiscover/AutoDiscover.xml"

If an HTTP Post to either of the above URIs results in an HTTP 302 redirect, then the redirect as found in the location field of the response is added to the list of possible AutoDiscover Server URIs. See section 2.2.3 of this document.

3.1.7 Locations Found from SRV DNS Records.

An AutoDiscover Client can query DNS for SRV records for the service. See section 2.2.2.

_autodiscover._tcp.<domain>

If the result is <host> then add “https://”<host>”AutoDiscover/AutoDiscover.xml” to the list of possible AutoDiscover URIs.

3.1.8 Locations Found by an HTTP Redirect.

An AutoDiscover Client can also issue an HTTP Get with the URI http://autodiscover.<domain>/autodiscover/autodiscover.xml.

If this URI results in an HTTP 302 redirect, then prompt the user warning them of the redirection. If the user accepts, then the new location is added to the list of possible AutoDiscover Server URIs.

3.2 Server Details

AutoDiscover Servers do not automatically publish all their locations. Administrators can manually publish AutoDiscover Server locations.

3.2.1 Locations Published in LDAP via Service Connection Points with an HTTP URI.

An administrator can publish a Service Connection Point to the following:

DN:<AdministratorChosenDN>
Changetype: add
Objectclass: serviceConnectionPoint
serviceBindingInformation: <AutoDiscoverServerURI>
Keywords: “”77378F46-2C66-4aa9-A6A6-3E7A48B19596”
<Extensions>

```
<Extensions> := NULL |
                Extension | Extensions

Extension := “Domain=” <AuthoritativeDomain> |
             “Site=” <ADSite>


<AuthoritativeDomain> is a domain that the AutoDiscoverServer can
provide information about.

<ADSite> is the AD Site as defined in [MS-ADTS]
```

3.2.2 Locations Published in LDAP via Service Connection Points with an LDAP URI.

If the administrator of the AutoDiscover Server knows that AutoDiscover Clients prefer a different LDAP server than the AutoDiscover Server, then the administrator can manually publish a Service Connection Point in the client's preferred LDAP server. A client querying for Service Connection Points can then learn about the AutoDiscover Server's preferred LDAP server.

DN:<AdministratorChosenDN>
Changetype: add
Objectclass: `serviceConnectionPoint`
`serviceBindingInformation: <LDAPURI>`
`Keywords: ""67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68"`
`<Extensions>`

```
<Extensions> := NULL |
                Extension | Extensions

Extension := "Domain=" <AuthoritativeDomain>


<AuthoritativeDomain> is a domain that the AutoDiscoverServer can
provide information about.
```

3.2.3 Locations Published in DNS as AutoDiscover.<Domain> and <Domain>

An administrator wanting to publish an AutoDiscover Server for <Domain> can configure DNS and SSL such that:

"https://AutoDiscover".<Domain>/AutoDiscover/AutoDiscover.xml and "https://<Domain>/AutoDiscover/AutoDiscover.xml are URIs serviced by AutoDiscover Servers.

This is configured manually.

3.2.4 Locations Published in DNS using SRV Records

If https://Server/Autodiscover/AutoDiscover.xml can serve AutoDiscover Clients for <Domain>, then an administrator can publish the following SRV Record.

SRV _autodiscover._tcp.<DOMAIN> = <AutoDiscoverServer>

This is configured manually. See section 2.2.2.

3.2.5 Locations Published through an HTTP GET

If https://Server/Autodiscover/AutoDiscover.xml can serve AutoDiscover Clients for <Domain>, then an administrator can configure the following HTTP Redirect.

HTTP://AutoDiscover.<Domain>/Autodiscover/AutoDiscover.xml to 302 redirect to https://Server/Autodiscover/AutoDiscover.xml

Non secure HTTP URIs SHOULD NOT be used to query settings as per [MS-OXDSCLI]. They SHOULD only be used for redirections.

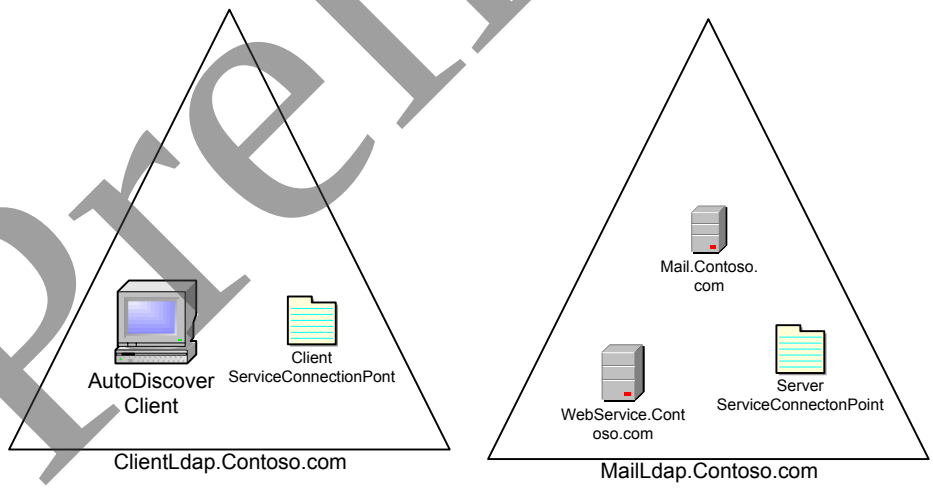
This is configured manually. See [RFC2616].

4 Protocol Examples

4.1 An AutoDiscover Server Publishing its Location

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
- The mailbox server and Web services server are configured to use MailLdap.Contoso.com as their LDAP server.
- Clients are configured to use ClientLdap.Contoso.Com



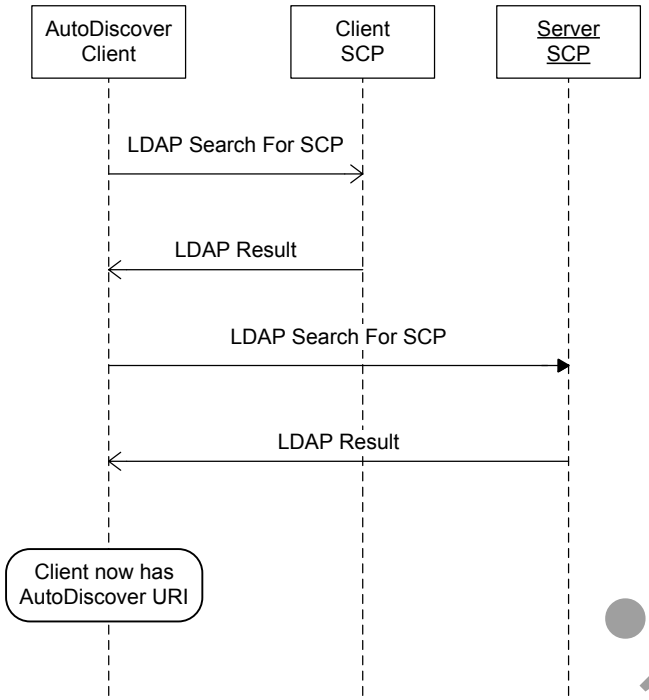
An administrator wants to publish AutoDiscover services for mailboxes on Mail.Contoso.com. For various reasons, the administrator is unable to configure https://contoso.com/AutoDiscover.AutoDiscover.xml to respond to AutoDiscover requests. Instead, the administrator uses [RFC1034] and [RFC2510] to create SSL certificates that allow the AutoDiscover Server to HTTP 302 redirect: https://AutoDiscover.Contoso.com/AutoDiscover/AutoDiscover.xml to https://WebService.Contoso.com/AutoDiscover/AutoDiscover.xml.

Also, the administrator creates and publishes two LDAP objects to help clients find the AutoDiscover Server.

MailLdap.Contoso.Com, the administrator publishes the following:
DN: CN=WebServices,CN=Autodiscover,CN=Protocols,CN=WebServices,CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=Contoso,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=Contoso,DC=com
Changetype: add
Objectclass: `serviceConnectionPoint`
`serviceBindingInformation:` https://WebService.Contoso.com/AutoDiscover/AutoDiscover.xml
`Keywords: “"77378F46-2C66-4aa9-A6A6-3E7A48B19596”`

On the client LDAP server, the administrator publishes the following:
DN: CN=mail.contoso.com,CN=Microsoft Exchange Autodiscover,CN=Services,CN=Configuration,DC=Users,DC=Contoso,DC=com
Changetype: add
Objectclass: `serviceConnectionPoint`
`serviceBindingInformation:` LDAP://MailLdap.Contoso.com
`Keywords: "67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68"`

4.2 An AutoDiscover Client Querying for AutoDiscover Servers



Assume the following configuration:

- A mail client is configured to use the e-mail address User@Contoso.com
- The mail client is configured to use ClientLdap.Contoso.Com as its LDAP server.
- Servers are configured as per section 3.1 of this document

The client wants to construct a list of URIs of possible AutoDiscover Server locations. First the client executes the steps found in section 2.1.3. The client searches its LDAP server on ClientLdap.Contoso.Com for a service connection points bearing the GUIDS `67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68` or `77378F46-2C66-4aa9-A6A6-3E7A48B19596`.

It does so by constructing the URI
LDAP//ClientLdap.Contoso.Com
"/?cn,serviceBindingInformation,Keywords?sub?(&(objectclass=`serviceConnectionPoint`)(|(keywords=67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68)(keywords=77378F46-2C66-4aa9-A6A6-3E7A48B19596)))"

After evaluating that query, the client is returned the object:

DN: CN=mail.contoso.com,CN=Microsoft Exchange Autodiscover,CN=Services,CN=Configuration,DC=Users,DC=Contoso,DC=com
Changetype: add
Objectclass: `serviceConnectionPoint`
`serviceBindingInformation:` LDAP://MailLdap.Contoso.com
`Keywords: "67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68"`

Seeing that the service binding information in an LDAP URI, the AutoDiscover Client then proceeds to construct the following:
LDAP//MailLdap.Contoso.Com
"/?cn,serviceBindingInformation,Keywords?sub?(&(objectclass=serviceConnectionPoint)(|(keywords=67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68)(keywords=77378F46-2C66-4aa9-A6A6-3E7A48B19596)))"

This query returns the following object:

DN:
CN=WebServices,CN=Autodiscover,CN=Protocols,CN=WebServices,CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=Contoso,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=Contoso,DC=com
Changetype: add
Objectclass: serviceConnectionPoint
serviceBindingInformation:
https://WebService.Contoso.com/AutoDiscover/AutoDiscover.xml
Keywords: ""77378F46-2C66-4aa9-A6A6-3E7A48B19596"

From this, the client adds https://WebService.Contoso.com/AutoDiscover/AutoDiscover.xml to the list of possible AutoDiscover Web Services.

Next, the client follows section 2.1.4 and adds the following:
https://AutoDiscover.Contoso.com/AutoDiscover/AutoDiscover.xml &
https://Contoso.com/AutoDiscover/AutoDiscover.xml to the list of possible email addresses.

As per section 2.2.2, the client executes a DNS search for the SRV record "_autodiscover._tcp.Contoso.com". No records are returned. This is expected behavior.

5 Security

5.1 Security Considerations for Implementers

There are many DNS spoofing attacks. For this reason, clients SHOULD NOT use non SSL URIs unless they have the consent of the user. Administrators MUST provide AutoDiscover data via HTTPS.

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.

Microsoft Windows Automatically preconfigures domain joined computers with an Active Directory Server. Outlook 2007 uses this LDAP server is used as the well known LDAP server.

Outlook 2007 uses the “ConfigurationNamingContext” of the pre-configured Active Directory Server as the well known distingquishedName for ServiceConnectionPoints.

7 Index