[MS-OXDISCO]: Autodiscover HTTP Service Protocol Specification

Revision Summary			
Author	Date	Version	Comments
Microsoft Corporation	April 4, 2008	0.1	Initial Availability.
Microsoft Corporation	June 27, 2008	1.0	Initial Release.
Microsoft Corporation	August 6, 2008	1.01	Updated references to reflect date of initial release.
Microsoft Corporation	September 3, 2008	1.02	Revised and edited technical content.

Table of Contents

1 Introduction

The Autodiscover HTTP Service Protocol extends the **Domain Name System (DNS)** and directory services to make the location and settings of mail servers available to clients in order to use the functionality specified in the Autodiscover Publishing and Lookup Protocol [MS-OXDSCLI].

1.1 Glossary

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

Active Directory (AD)
Autodiscover client
Autodiscover server
common name (CN)
distinguished name (DN)
Domain Name System (DNS)
GUID
Hypertext Transfer Protocol (HTTP)
Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)
LDAP server
Lightweight Directory Access Protocol (LDAP)
Secure Sockets Layer (SSL)
Service Connection Point (SCP)
Uniform Resource Identifier (URI)
XML

The following terms are specific to this document:

Autodiscover directory service map GUID: The **GUID** value `67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68`, which identifies **SCP** objects that identify other directory service forests that MAY contain **Autodiscover server** information.

Autodiscover URI map GUID: The GUID value `77378F46-2C66-4aa9-A6A6-3E7A48B19596`, which identifies **SCP** objects that identify **Autodiscover server** URIs.

LDAP Data Interchange Format (LDIF): An Internet Engineering Task Force (IETF) standard that defines how to import and export directory data between directory servers that use LDAP service providers. For more details, see [RFC2849].

port: A TCP IP **port**. For more details, see [RFC814] section 6.

service binding information: The **URI** needed to bind to a service.

SRV record: A DNS resource record that is used to identify computers that host specific services.

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-OXDSCLI] Microsoft Corporation, "Autodiscover Publishing and Lookup Protocol Specification", June 2008.

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

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

[RFC1558] Howes, T., "A String Representation of LDAP Search Filters", RFC 1558, December 1993, http://www.ietf.org/rfc/rfc1558.txt.

[RFC1823] Howes, T. and Smith, M., "The LDAP Application Program Interface", RFC 1823, August 1995, http://www.ietf.org/rfc/rfc1823.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.

[RFC2396] Berners-Lee, T., Fielding, R., and Masinter, L., "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998, http://www.ietf.org/rfc/rfc2396.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.

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

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

[RFC814] Clark, David D., "NAME, ADDRESSES, PORTS, AND ROUTES", RFC 814, July 1982, http://www.ietf.org/rfc/rfc0814.txt.

1.2.2 Informative References

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

[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

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

Uniform resource identifiers (URI) for Autodiscover server locations can be published using the following methods:

- **Service Connection Point (SCP)** objects which can be queried by using the **Lightweight Directory Access Protocol (LDAP)**
- Direct **DNS** configuration
- DNS service (SRV) record configuration
- **Hypertext Transfer Protocol over Secure Socket Layer (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, as specified in [MS-OXDSCLI]. This protocol relies on **HTTPS,** as specified in [RFC2818], for data protection services and it relies on [RFC1034] for **DNS** services. It also relies on [MS-ADTS] and [RFC1823] for the **SCP** object and **LDAP**, respectively.

The following data flow diagram shows a client querying the directory and the DNS for an Autodiscover server, and the server publishing its location in the directory and DNS.

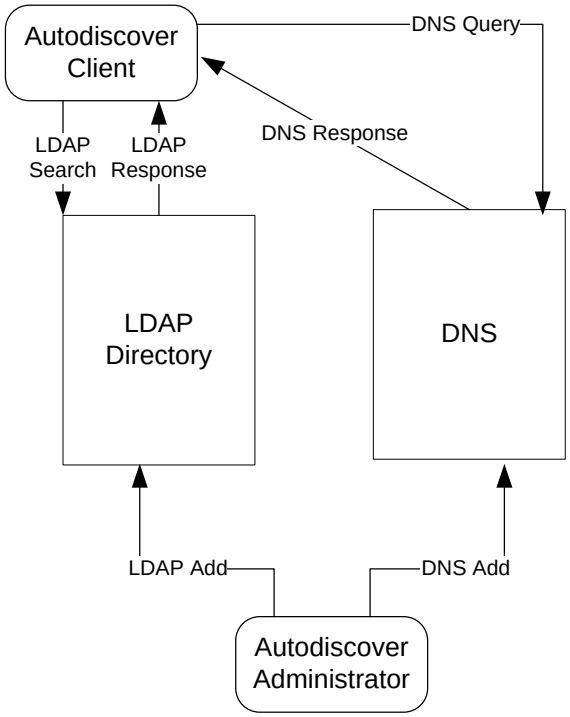

Figure 1: Autodiscover client and server interactions

1.5 Prerequisites/Preconditions

The **Autodiscover client** SHOULD be configured with an **LDAP** directory and base **distinguished name (DN)** that is well-known to the **Autodiscover server** administrator.

The Autodiscover server SHOULD be configured with a **Secure Sockets Layer (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.<1>

The following transports and data sources are used:

1. **LDAP** and LDAP directories. For more details, see [RFC1823].
2. The **DNS** and DNS SRV records. For more details, see [RFC1034] and [RFC2782].
3. **Hypertext Transfer Protocol (HTTP)** and HTTP 302 redirection. For more details, see [RFC2616].

2.2 Message Syntax

2.2.1 SCP Publication Service Objects

2.2.1.1 LDIF Format

Using the formal syntax definition of the **LDAP Data Interchange Format (LDIF)** as specified in [RFC2849], an SCP can be expressed as the following:

```
DN: <distingushedName>
Objectcategory: serviceConnectionPoint
Keyword: <KeywordValue>
[Keyword: <KeywordValue>]
ServiceBindingInformation:<serviceBindingInformationValue>
```

That is, an **SCP** object MUST have a <distinguishedName>, one or more <KeywordValue>, and one <serviceBindingInformationValue>.

2.2.1.2 Searching 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 the <host>. This value is commonly 389. This value SHOULD be well-known to the Autodiscover client and Autodiscover server administrator.
- <DN> is the **distinguished name (DN)** 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, the value MUST be LDAP_SCOPE_SUBTREE. This is a constant specified in [RFC1823] section 4.4.

- The list of attributes to query. For the purposes of this protocol, the list MUST contain "ServiceBindingInformation", and "Keywords".
- An LDAP search filter, as specified in [RFC1558]. For the purposes of this protocol, <filter> is

```
(&(objectcategory=serviceConnectionPoint)(|(keywords=67661D7F-8FC4-
4fa7-BFAC-E1D7794C1F68)( keywords=77378F46-2C66-4aa9-A6A6-
3E7A48B19596)))
```

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

2.2.1.3 Creating SCP Objects

SCP objects 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 the <host>. This value is typically 389. This value SHOULD be well-known to the Autodiscover client and Autodiscover server administrator.
- A DN 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 the purposes of this protocol, the list MUST contain "ServiceBindingInformation", and "Keywords"
- The list of "ServiceBindingInformation" and the "Keywords" attribute values. For more information, see section 3.1.5.1 and 3.2.3.1.
- The <objectcategory> to create. For the purposes of this protocol, the object category MUST be "ServiceConnectionPoint".

2.2.2 DNS SRV Queries

To query for **Autodiscover servers**, the **Autodiscover client** SHOULD use the following data elements specified by 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. If no valid entries are found, then the query will return an empty list.

2.2.3 HTTP 302 Redirection

The following section uses Augmented Backus-Naur Form (ABNF) notation. For more details, see [RFC5234].

The **Autodiscover client** MAY send an **HTTP** GET request to retrieve the Request-Uri. The Request-Uri has the following format:

```
<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.

The <RequestUri> can be processed as specified in [RFC2616], section 9.3. If the response is a 302 redirection (as specified in [RFC2616] section 10.3.3), the Autodiscover client uses the value of the redirection URL. Note that if the response is not a 302 redirection, then the expected response is an **Autodiscover server** URI.

2.2.4 E-mail Addresses

All e-mail addresses are assumed to be in the format specified in [RFC2822] section 3.4.1. That is, they follow the format <local-part> "@" <domain>.

2.2.5 Autodiscover Server URI Results

The result of an Autodiscover query is a list of possible **Autodiscover server** URIs. **URIs** are specified in [RFC3986].

3 Protocol Details

This protocol specifies a way for **Autodiscover clients** to find **Autodiscover servers**. The client 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

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 that described in this document.

The main data elements required by any implementation are :

- **E-mail address:** An e-mail address of the form <local-part> @ <domain>. This is the e-mail address for which the corresponding **Autodiscover server** URI is being located.
- **LDAP directories and SCP objects: LDAP** directories contain published server locations in **SCP** objects**.** The SCP object can be used to identify Autodiscover server URIs.
- **DNS & DNS SRV records: DNS** MAY contain **SRV records** for the Autodiscover service. The SRV records can then be used to find the Autodiscover server URI.

3.1.2 Timers

None.

3.1.3 Initialization

The client requires an e-mail address of the form <local-part> "@" <domain>.

3.1.4 Higher-Layer Triggered Events

The Autodiscover publishing and lookup services are triggered by a user action, or optionally a timer.

3.1.5 Message Processing Events and Sequencing Rules

The **Autodiscover client** expands the e-mail address provided during initialization into a list of URIs as specified in [RFC2396]. Since **Autodiscover server** URIs can be acquired in different ways, to create a fully-populated list, the Autodiscover client SHOULD do all of the following:

- Query a well-known **LDAP server** for **SCP** objects, as described in section 3.1.5.1.
- Perform text manipulations on the domain of the email address, as described in section 3.1.5.2.
- Search the **DNS** for Autodiscover **SRV records**, as described in section 3.1.5.3.
- Perform an **HTTP** GET request to determine whether there are redirects to other **Autodiscover servers**, as described in section 3.1.5.4.

Note that a client can acquire the URI of an Autodiscover server without a fully-populated list of Autodiscover server URIs.

3.1.5.1 Query an Well-Known LDAP Server for SCP objects

Autodiscover server locations can be published in **LDAP** directories via **SCP** objects.

To discover these servers, **Autodiscover client**s 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 **ServiceBindingInformation** attribute is an "HTTP://" or HTTPS:// URI then the client has found a URI that is possibly an **Autodiscover server** and the client SHOULD add 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.

3.1.5.2 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. For more details, see section 2.2.3. For more details about Autodiscover client requests, see [MS-OXDISCCLI] section 3.1.7.1.

3.1.5.3 Locations Found from SRV DNS Records.

An **Autodiscover client** can query **DNS** for **SRV records** for the Autodiscover service using the following command. For more information, 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**.

3.1.5.4 Locations Found by an HTTP Redirect.

An **Autodiscover client** can also issue an **HTTP** GET method with the **URI** set to 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.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

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 that described in this document.

The main data elements required by any implementation are :

- **Published Autodiscover server URIs:** Servers MUST have published locations in order for clients to find them using the Autodiscover service.

3.2.2 Timers

None.

3.2.3 Initialization

Autodiscover servers do not automatically publish all their locations. Administrators can manually publish Autodiscover server locations.

3.2.3.1 Locations Published in LDAP via SCP Objects with an HTTP URI

An administrator can publish an **SCP** object using the following values:

```
DN:<AdministratorChosenDN>
Changetype: add
Objectcategory: 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 Autodiscover server can provide information about.

<ADSite> is the AD Site as specified in [MS-ADTS].

3.2.3.2 Locations Published in LDAP via SCP objects with an LDAP URI.

If the administrator of the **Autodiscover server** knows that **Autodiscover client**s prefer a different **LDAP server** than the Autodiscover server, then the administrator can manually publish an **SCP** object in the client's preferred LDAP server. A client querying for **SCP** objects can then learn about the Autodiscover server's preferred LDAP server.

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

<Extensions> := NULL |
                Extension | Extensions

Extension := "Domain=" <AuthoritativeDomain>
```

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

3.2.3.3 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.

3.2.3.4 Locations Published in DNS using SRV Records

If https://Server/Autodiscover/Autodiscover.xml can serve **Autodiscover client**s for the given <Domain>, then an administrator can publish the following **SRV record**.

```
SRV _autodiscover._tcp.<DOMAIN> = <AutodiscoverServer>
```

This is configured manually. See section 2.2.2.

3.2.3.5 Locations Published through an HTTP GET

If https://Server/Autodiscover/Autodiscover.xml can serve **Autodiscover client**s 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 specified in [MS-OXDSCLI]. They SHOULD only be used for redirections.

This is configured manually. For more details, see [RFC2616].

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.

4 Protocol Examples

4.1 Publishing an Autodiscover Server 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

The following figure illustrates the topology.

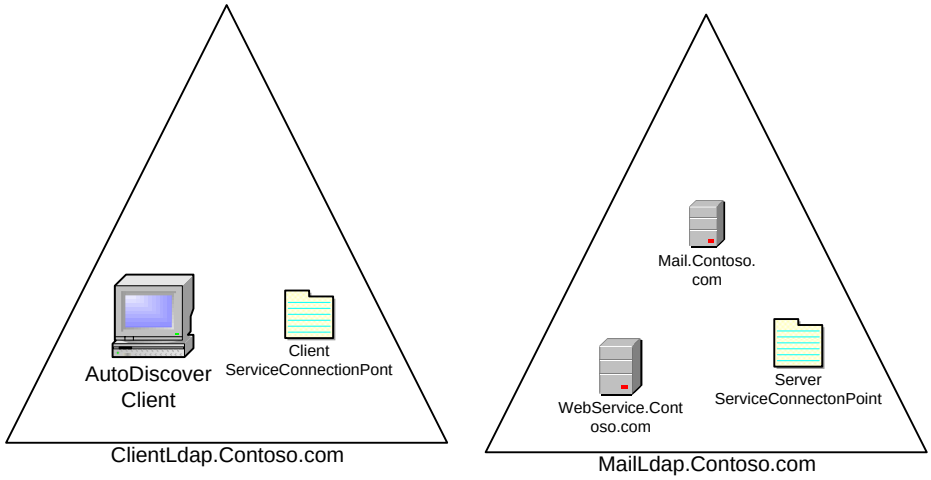

Figure 2: Topology of Autodiscover client and server

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.

For MailLdap.Contoso.Com, the administrator publishes the following:

```
DN:
CN=WebServices,CN=Autodiscover,CN=Protocols,CN=WebServices,CN=Servers,CN=Ex
change Administrative Group (FYDIBOHF23SPDLT),CN=Administrative
Groups,CN=Contoso,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=Contoso,DC=com
Changetype: add
Objectcategory: 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
Objectcategory: 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 specified in section 3.2 of this document.

The client wants to construct a list of **URIs** of possible **Autodiscover server** locations. First the client executes the steps specified in section 3.1.5.1. The client searches its LDAP server on ClientLdap.Contoso.Com for an **SCP** object bearing the following **GUIDs:** 67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68 or 77378F46-2C66-4aa9-A6A6-3E7A48B19596.

The client performs the search by constructing the following URI:

```
LDAP//ClientLdap.Contoso.Com
"/?cn,serviceBindingInformation,Keywords?sub?(&(objectcategory=serviceConne
ctionPoint)(|(keywords=67661D7F-8FC4-4fa7-BFAC-E1D7794C1F68)(
keywords=77378F46-2C66-4aa9-A6A6-3E7A48B19596)))"
```

After evaluating that query, the following **SCP** object is returned to the client:

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

Seeing that the service binding information is provided in an **LDAP** URI, the **Autodiscover client** then proceeds to construct the following:

```
LDAP//MailLdap.Contoso.Com
"/?cn,serviceBindingInformation,Keywords?sub?(&(objectcategory=serviceConne
ctionPoint)(|(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=Ex
change Administrative Group (FYDIBOHF23SPDLT),CN=Administrative
Groups,CN=Contoso,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=Contoso,DC=com
Changetype: add
Objectcategory: 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.

The communication is shown in the following figure.

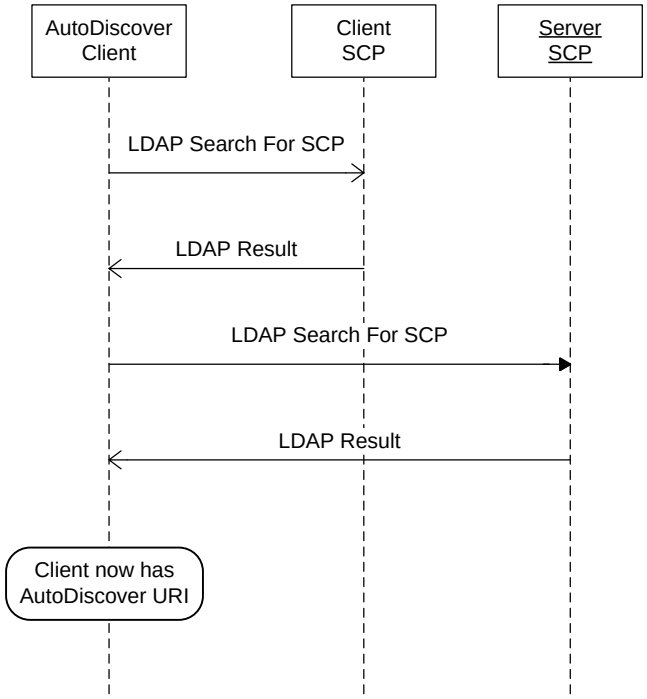

Figure 3: Communication required to find an Autodiscover server URI using SCP objects

Next, the client adds https://Autodiscover.Contoso.com/Autodiscover/Autodiscover.xml & https://Contoso.com/Autodiscover/Autodiscover.xml to the list of possible email addresses based on the information specified in section 3.1.5.2.

As specified in section 2.2.1.2, 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 possible **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.

<1> Section 2.1: Microsoft Windows automatically pre-configures domain joined computers with an **Active Directory (AD)** server. Outlook 2007 SP1 uses this **LDAP server** as the well-known LDAP server. Outlook 2007 SP1 uses the **ConfigurationNamingContext** of the pre-configured Active Directory server as the well-known **DN** for **SCP** objects.

Index