

# [MS-OCDISCWS]:

## Lync Autodiscover Web Service Protocol

---

### Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation (“this documentation”) for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft [Open Specifications Promise](#) or the [Microsoft Community Promise](#). If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting [iplg@microsoft.com](mailto:iplg@microsoft.com).
- **License Programs.** To see all of the protocols in scope under a specific license program and the associated patents, visit the [Patent Map](#).
- **Trademarks.** The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit [www.microsoft.com/trademarks](http://www.microsoft.com/trademarks).
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

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

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

**Support.** For questions and support, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

## Revision Summary

Date	Revision History	Revision Class	Comments
1/20/2012	0.1	New	Released new document.
4/11/2012	0.1	None	No changes to the meaning, language, or formatting of the technical content.
7/16/2012	0.1	None	No changes to the meaning, language, or formatting of the technical content.
10/8/2012	1.0	Major	Significantly changed the technical content.
2/11/2013	2.0	Major	Significantly changed the technical content.
7/30/2013	2.1	Minor	Clarified the meaning of the technical content.
11/18/2013	2.1	None	No changes to the meaning, language, or formatting of the technical content.
2/10/2014	2.1	None	No changes to the meaning, language, or formatting of the technical content.
4/30/2014	2.2	Minor	Clarified the meaning of the technical content.
7/31/2014	3.0	Major	Significantly changed the technical content.
10/30/2014	3.0	None	No changes to the meaning, language, or formatting of the technical content.
3/30/2015	4.0	Major	Significantly changed the technical content.
9/4/2015	4.0	None	No changes to the meaning, language, or formatting of the technical content.
7/15/2016	4.0	None	No changes to the meaning, language, or formatting of the technical content.
9/14/2016	4.0	None	No changes to the meaning, language, or formatting of the technical content.
4/27/2018	5.0	Major	Significantly changed the technical content.
7/24/2018	6.0	Major	Significantly changed the technical content.
8/28/2018	7.0	Major	Significantly changed the technical content.
12/11/2018	7.1	Minor	Clarified the meaning of the technical content.

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	Glossary	5
1.2	References	6
1.2.1	Normative References	6
1.2.2	Informative References	7
1.3	Overview	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	7
1.9	Standards Assignments	7
<b>2</b>	<b>Messages</b>	<b>8</b>
2.1	Transport	8
2.2	Message Syntax	8
2.2.1	Namespaces	8
2.2.2	Custom HTTP Headers	8
2.2.2.1	Authorization Header	8
2.2.2.2	X-Ms-WebTicket Header	9
2.2.2.3	X-Ms-WebTicketUrl Header	9
2.2.3	Common URI Parameters	9
2.2.3.1	Sipuri URI Parameter	9
2.2.4	Complex Types	9
2.2.4.1	AutodiscoverResponse	10
2.2.4.2	Domain	11
2.2.4.3	Link	12
2.2.4.4	Root	12
2.2.4.5	SipAccess	13
2.2.4.6	User	14
2.2.5	Attributes	15
2.2.5.1	AccessLocation	16
2.2.5.2	Fqdn	16
2.2.5.3	Href	16
2.2.5.4	Port	16
2.2.5.5	Token	16
<b>3</b>	<b>Protocol Details</b>	<b>18</b>
3.1	Server Details	18
3.1.1	Abstract Data Model	18
3.1.2	Timers	18
3.1.3	Initialization	18
3.1.4	Higher-Layer Triggered Events	18
3.1.5	Message Processing Events and Sequencing Rules	18
3.1.5.1	Common Processing Details	18
3.1.5.2	Root	19
3.1.5.2.1	GET	19
3.1.5.2.1.1	Request Body	19
3.1.5.2.1.2	Response Body	19
3.1.5.3	User	19
3.1.5.3.1	GET	20
3.1.5.3.1.1	Request Body	20
3.1.5.3.1.2	Response Body	20
3.1.5.4	Domain	20
3.1.5.4.1	GET	21

3.1.5.4.1.1	Request Body .....	21
3.1.5.4.1.2	Response Body .....	21
3.1.5.5	OAuth.....	21
3.1.5.5.1	GET .....	22
3.1.5.5.1.1	Request Body .....	22
3.1.5.5.1.2	Response Body .....	22
3.1.6	Timer Events.....	22
3.1.7	Other Local Events.....	22
3.2	Client Details .....	22
3.2.1	Abstract Data Model .....	22
3.2.1.1	Discovery of Autodiscover .....	22
3.2.1.2	Redirect Detection.....	23
3.2.1.3	Internal External Network Switching .....	23
3.2.2	Timers .....	23
3.2.3	Initialization.....	23
3.2.4	Higher-Layer Triggered Events .....	23
3.2.5	Message Processing Events and Sequencing Rules .....	23
3.2.6	Timer Events.....	23
3.2.7	Other Local Events.....	23
<b>4</b>	<b>Protocol Examples .....</b>	<b>24</b>
4.1	Discover Home Server .....	24
<b>5</b>	<b>Security .....</b>	<b>27</b>
5.1	Security Considerations for Implementers .....	27
5.2	Index of Security Parameters .....	27
<b>6</b>	<b>Appendix A: Full XML Schema.....</b>	<b>28</b>
<b>7</b>	<b>Appendix B: Full JSON Schema .....</b>	<b>29</b>
<b>8</b>	<b>Appendix C: Product Behavior .....</b>	<b>31</b>
<b>9</b>	<b>Change Tracking.....</b>	<b>32</b>
<b>10</b>	<b>Index.....</b>	<b>33</b>

# 1 Introduction

The Lync Autodiscover Web Service Protocol defines a set of operations that allows a client to discover its home server information.

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

## 1.1 Glossary

This document uses the following terms:

**200 OK:** A response to indicate that the request has succeeded.

**byte order mark:** A Unicode character that is used to indicate that text is encoded in UTF-8, UTF-16, or UTF-32.

**fully qualified domain name (FQDN):** An unambiguous domain name that gives an absolute location in the Domain Name System's (DNS) hierarchy tree, as defined in [\[RFC1035\]](#) section 3.1 and [\[RFC2181\]](#) section 11.

**Hypertext Markup Language (HTML):** An application of the Standard Generalized Markup Language (SGML) that uses tags to mark elements in a document, as described in [\[HTML\]](#).

**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 Secure (HTTPS):** An extension of HTTP that securely encrypts and decrypts web page requests. In some older protocols, "Hypertext Transfer Protocol over Secure Sockets Layer" is still used (Secure Sockets Layer has been deprecated). For more information, see [\[SSL3\]](#) and [\[RFC5246\]](#).

**JavaScript Object Notation (JSON):** A text-based, data interchange format that is used to transmit structured data, typically in Asynchronous JavaScript + XML (AJAX) web applications, as described in [\[RFC7159\]](#). The JSON format is based on the structure of ECMAScript (Jscript, JavaScript) objects.

**Session Initiation Protocol (SIP):** An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. **SIP** is defined in [\[RFC3261\]](#).

**topology:** The structure of the connections between members.

**Uniform Resource Identifier (URI):** A string that identifies a resource. The URI is an addressing mechanism defined in Internet Engineering Task Force (IETF) Uniform Resource Identifier (URI): Generic Syntax [\[RFC3986\]](#).

**Uniform Resource Locator (URL):** A string of characters in a standardized format that identifies a document or resource on the World Wide Web. The format is as specified in [\[RFC1738\]](#).

**UTF-8:** A byte-oriented standard for encoding Unicode characters, defined in the Unicode standard. Unless specified otherwise, this term refers to the UTF-8 encoding form specified in [\[UNICODE5.0.0/2007\]](#) section 3.9.

**XML namespace:** A collection of names that is used to identify elements, types, and attributes in XML documents identified in a URI reference [\[RFC3986\]](#). A combination of XML namespace and local name allows XML documents to use elements, types, and attributes that have the same names but come from different sources. For more information, see [\[XMLNS-2ED\]](#).

**XML schema:** A description of a type of XML document that is typically expressed in terms of constraints on the structure and content of documents of that type, in addition to the basic syntax constraints that are imposed by XML itself. An XML schema provides a view of a document type at a relatively high level of abstraction.

**MAY, SHOULD, MUST, SHOULD NOT, MUST NOT:** These terms (in all caps) are used as defined in [\[RFC2119\]](#). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

## 1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the [Errata](#).

### 1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com). We will assist you in finding the relevant information.

[MS-OCAUTHWS] Microsoft Corporation, "[OC Authentication Web Service Protocol](#)".

[MS-OCSMP] Microsoft Corporation, "[Microsoft Online Conference Scheduling and Management Protocol](#)".

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

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

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

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and Schooler, E., "SIP: Session Initiation Protocol", RFC 3261, June 2002, <http://www.ietf.org/rfc/rfc3261.txt>

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

[RFC4627] Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)", RFC 4627, July 2006, <http://www.rfc-editor.org/rfc/rfc4627.txt>

[WS-MetaDataExchange] Ballinger, K. et al., "Web Services Metadata Exchange (WS-MetadataExchange) Version 1.1", August 2006, <http://specs.xmlsoap.org/ws/2004/09/mex/WS-MetadataExchange.pdf>

[XMLNS] Bray, T., Hollander, D., Layman, A., et al., Eds., "Namespaces in XML 1.0 (Third Edition)", W3C Recommendation, December 2009, <http://www.w3.org/TR/2009/REC-xml-names-20091208/>

[XMLSCHEMA1/2] Thompson, H., Beech, D., Maloney, M., and Mendelsohn, N., Eds., "XML Schema Part 1: Structures Second Edition", W3C Recommendation, October 2004, <http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/>

[XMLSCHEMA2/2] Biron, P., and Malhotra, A., Eds., "XML Schema Part 2: Datatypes Second Edition", W3C Recommendation, October 2004, <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>

## 1.2.2 Informative References

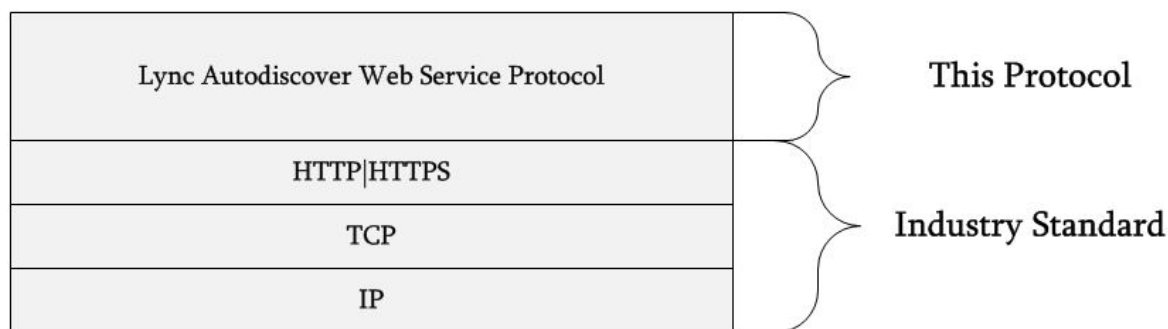
None.

## 1.3 Overview

This protocol allows clients to discover web services on their home server and general topology information.

## 1.4 Relationship to Other Protocols

This protocol uses **Hypertext Transfer Protocol (HTTP)**, as described in [\[RFC2616\]](#), and **Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)**, as described in [\[RFC2818\]](#), as shown in the following layering diagram.



**Figure 1: This protocol in relation to other protocols**

This protocol is dependent on [\[MS-OCAUTHWS\]](#) to authenticate users.

## 1.5 Prerequisites/Preconditions

Prior to the protocol execution, it is required that DNS entries be configured for both the internal and external Autodiscover services. The DNS entries are canonical name entries of the format `lyncdiscover.<sipdomain>` and `lyncdiscoverinternal.<sipdomain>` whose entries point to the primary Autodiscover service for the deployment's **Session Initiation Protocol (SIP)** domain. These DNS entries will allow the protocol client to discover the first-hop Autodiscover service in the protocol execution. Further client details are described in section [3.2](#).

## 1.6 Applicability Statement

This protocol is applicable to clients that need to discover their home server information.

## 1.7 Versioning and Capability Negotiation

None.

## 1.8 Vendor-Extensible Fields

None.

## 1.9 Standards Assignments

None.

## 2 Messages

### 2.1 Transport

Protocol messages MUST be transported via **HTTP**, as specified in [\[RFC2616\]](#), or **HTTPS**, as specified in [\[RFC2818\]](#). The service SHOULD be served on ports 80 and 443, but MAY be served on other ports.

Protocol messages are text-based and MUST be **UTF-8** encoded. Messages MUST NOT contain a **byte order mark**.

### 2.2 Message Syntax

This section contains common definitions used by this protocol. The syntax of the definitions uses the **XML schema** as defined in [\[XMLSCHEMA1/2\]](#) and [\[XMLSCHEMA2/2\]](#), and **JavaScript Object Notation (JSON)** as specified in [\[RFC4627\]](#).

#### 2.2.1 Namespaces

This specification defines and references various **XML namespaces** using the mechanisms specified in [\[XMLNS\]](#). Although this specification associates a specific XML namespace prefix for each XML namespace that is used, the choice of any particular XML namespace prefix is implementation-specific and not significant for interoperability.

Prefix	Namespaces URI	Reference
xs	<a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a>	<a href="#">[XMLSCHEMA1/2]</a> <a href="#">[XMLSCHEMA2/2]</a>

#### 2.2.2 Custom HTTP Headers

The messages exchanged in this protocol use the following HTTP headers in addition to the existing set of standard HTTP headers.

Header	Description
Authorization	Specifies the client authentication header for requests to the OAuth Resource defined in section <a href="#">3.1.5.5</a> .
X-Ms-WebTicket	Specifies the client authentication header for requests to the User Resource defined in section <a href="#">3.1.5.3</a> .
X-Ms-WebTicketUrl	Specifies the Web Ticket Service location where a client can retrieve the web ticket. The Web Ticket Service is described in <a href="#">[MS-OAUTHWS]</a> .

##### 2.2.2.1 Authorization Header

The request to the OAuth resource MUST contain this authorization header. If the request does not include the authorization header, the request will be rejected with a 401 Unauthorized error code. The semantics regarding this authorization header are specified in [\[RFC2616\]](#) section 14.8 and more details about this authorization header are described in [\[MS-OAUTHWS\]](#).



### 2.2.2.2 X-Ms-WebTicket Header

The request to the User resource MUST contain the X-Ms-WebTicket header. If the request does not include this header, the request will be rejected with a 401 Unauthorized error code. The semantics regarding this header are specified in [\[MS-OCAUTHWS\]](#).

### 2.2.2.3 X-Ms-WebTicketUrl Header

If the request to the User resource does not contain an X-Ms-WebTicket header, the 401 Unauthorized response will contain the X-Ms-WebTicketUrl header with the value being the **URL** of the Web Ticket Service, as described in [\[MS-OCAUTHWS\]](#). The semantics regarding this header are specified as follows:

```
X-Ms-WebTicketUrl = "X-Ms-WebTicketUrl" ":" absolute-URI
```

The semantics regarding absolute-URI are specified in [\[RFC3986\]](#) section 4.3.

## 2.2.3 Common URI Parameters

The following table summarizes the set of common **URI** parameters defined by this specification.

URI parameter	Description
sipuri	The <b>Session Initiation Protocol (SIP)</b> URI of the user whose home server information is being discovered.

### 2.2.3.1 Sipuri URI Parameter

The request to the root resource MUST contain the *sipuri* parameter, as specified in [\[RFC3261\]](#) section 25.1<1>. If the request does not contain this parameter, the client MAY eventually receive a 404 Not Found response code when proceeding with the rest of the protocol.

## 2.2.4 Complex Types

The following table summarizes the set of common **XML schema** complex type definitions defined by this specification. XML schema complex type definitions that are specific to a particular operation are described with the operation.

Complex Type	Description
AutodiscoverResponse	The type of the top level element <b>AutodiscoverResponse</b> that will always be returned in every Autodiscover response.
Domain	Contains links that define topology information of the current server.
Link	Contains an <b>href</b> attribute which indicates the <b>URL</b> to access the resource identified by its corresponding token attribute.
Root	Contains a collection of links that identify resources exposed by the current server.
SipAccess	Contains the <b>fully qualified domain name (FQDN)</b> and port of the <b>Session Initiation Protocol (SIP)</b> server.

Complex Type	Description
User	Contains topology information of the user's home server.

### 2.2.4.1 AutodiscoverResponse

The **AutodiscoverResponse** type is the type of the top level element **AutodiscoverResponse** that **MUST** be returned in every Autodiscover response where a body is present. This type **MUST** contain one and only one of the possible sub-elements: **Domain** (see the **Domain** type, section [2.2.4.2](#)), **Root** (see the **Root** type, section [2.2.4.4](#)), or **User** (see the **User** type, section [2.2.4.6](#)).

The **AccessLocation** attribute **MUST** be present, as specified in section [2.2.5.1](#).

XML Schema:

```
<xs:complexType name="AutodiscoverResponse">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="1" name="Root" type=" Root"/>
    <xs:element minOccurs="0" maxOccurs="1" name="User" type=" User"/>
    <xs:element minOccurs="0" maxOccurs="1" name="Domain" type=" Domain"/>
  </xs:sequence>
  <xs:attribute name="AccessLocation" type="xs:string"/>
</xs:complexType>
```

JSON Schema:

```
AutodiscoverResponse
{
  "id": " AutodiscoverResponse",
  "type": "object",
  "properties": {
    "AccessLocation": {
      "required": true,
      "type": [
        "string",
        "null"
      ]
    },
    "Root": {
      "id": "Root",
      "required": true,
      "type": [
        "object",
        "null"
      ]
    },
    "User": {
      "id": "User",
      "required": true,
      "type": [
        "object",
        "null"
      ]
    },
    "Domain": {
      "id": "Domain",
      "required": true,
```

```

        "type": [
            "object",
            "null"
        ],
    }
}

```

## 2.2.4.2 Domain

The **Domain** type contains links that define topology information of the current server.

There is also a collection of links contained in the **Domain** type. These **Link** (see the **Link** type, section [2.2.4.3](#)) elements indicate the web service URL for the corresponding tokens. The possible tokens are defined in section [3.1.5.4](#).

Information regarding the **SipAccess** type is in section [2.2.4.5](#).

XML Schema:

```

<xs:complexType name="Domain">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="1" name="SipServerInternalAccess" type="SipAccess" />
    <xs:element minOccurs="0" maxOccurs="1" name="SipClientInternalAccess" type="SipAccess" />
    <xs:element minOccurs="0" maxOccurs="1" name="SipServerExternalAccess" type="SipAccess" />
    <xs:element minOccurs="0" maxOccurs="1" name="SipClientExternalAccess" type="SipAccess" />
    <xs:element minOccurs="0" maxOccurs="unbounded" name="Link" type="Link"/>
  </xs:sequence>
</xs:complexType>

```

JSON Schema:

```

"Domain": {
  "id": " Domain",
  "required": true,
  "type": [
    "object",
    "null"
  ],
  "properties": {
    "SipServerInternalAccess": {
      "$ref": "SipAccess"
    },
    "SipClientInternalAccess": {
      "$ref": "SipAccess"
    },
    "SipServerExternalAccess": {
      "$ref": "SipAccess"
    },
    "SipClientExternalAccess": {
      "$ref": "SipAccess"
    },
    "Links": {
      "$ref": "Link[]"
    }
  }
}

```

### 2.2.4.3 Link

The **Link** type is used to identify the URL to access a server resource. The URL which the **Link** element gives access to is present in the **href** attribute. The **token** attribute of the link is a unique string that identifies the type of resource to which the corresponding href will give access. The **token** (section [2.2.5](#)) and **href** (section [2.2.5](#)) attributes MUST be present in every **Link** element. For more details about **token**, see section [2.2.5.5](#).

XML Schema:

```
<xs:complexType name="Link">
  <xs:attribute name="token" type="xs:string"/>
  <xs:attribute name="href" type="xs:string"/>
</xs:complexType>
```

JSON Schema:

```
"items": {
  "id": "Link",
  "type": [
    "object",
    "null"
  ],
  "properties": {
    "token": {
      "required": true,
      "type": [
        "string",
        "null"
      ]
    },
    "href": {
      "required": true,
      "type": [
        "string",
        "null"
      ]
    }
  }
}
```

### 2.2.4.4 Root

The **Root** type contains links that define URLs that are served by the responding Autodiscover service. See the **Link** type in section [2.2.4.3](#) for the **Link** element. The corresponding tokens that identify these links are defined in section [3.1.5.2](#).

XML Schema:

```
<xs:complexType name="Root">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="unbounded" name="Link" type="Link"/>
  </xs:sequence>
</xs:complexType>
```

JSON Schema:

```

"Root": {
  "id": "Root",
  "required": true,
  "type": [
    "object",
    "null"
  ],
  "properties": {
    "Links": {
      "id": "Link[]",
      "required": true,
      "type": [
        "array",
        "null"
      ],
      "items": {
        "id": "Link",
        "type": [
          "object",
          "null"
        ],
        "properties": {
          "token": {
            "required": true,
            "type": [
              "string",
              "null"
            ]
          },
          "href": {
            "required": true,
            "type": [
              "string",
              "null"
            ]
          }
        }
      }
    }
  }
}

```

### 2.2.4.5 SipAccess

The **SipAccess** type reveals the **fully qualified domain name (FQDN)** and port of the **Session Initiation Protocol (SIP)** server. Protocol clients can use the **fqdn** and **port** attributes to connect to the SIP server front-end. See section [2.2.5](#) for the **fqdn** and **port** attributes. The **SipAccess** type is contained in the User and Domain resources under the elements. The type can be defined in four different elements that give different meanings to how the contents SHOULD be used. The behavior is described in the following table:

Type	Description
SipServerInternalAccess	This element reveals the SIP server FQDN and listening port to be used by SIP servers in the internal network.
SipServerExternalAccess	This element defines the SIP server FQDN and listening port to be used by SIP servers in the external network.
SipClientInternalAccess	This element defines the SIP server FQDN and listening port to be used by SIP clients in the internal network.
SipClientExternalAccess	This element defines the SIP server FQDN and listening port to be used by SIP clients in the external network.

## XML Schema:

```
<xs:complexType name="SipAccess">
  <xs:attribute name="fqdn" type="xs:string" />
  <xs:attribute name="port" type="xs:string" />
</xs:complexType>
```

## JSON Schema:

```
"properties": {
  "SipAccess": {
    "id": "SipAccess",
    "required": true,
    "type": [
      "object",
      "null"
    ],
  },
  "properties": {
    "fqdn": {
      "required": true,
      "type": [
        "string",
        "null"
      ]
    },
    "port": {
      "required": true,
      "type": [
        "string",
        "null"
      ]
    }
  }
}
```

### 2.2.4.6 User

The **User** type contains links that define topology information for the current user.

There is also a collection of links contained in the **User** type. These **link** (see the **Link** type in section [2.2.4.3](#)) elements indicate the web service URL for the corresponding tokens. The possible tokens are defined in section [3.1.5.3](#).

Information regarding the **SipAccess** type is found in section [2.2.4.5](#).

## XML Schema:

```
<xs:complexType name="User">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="1" name="SipServerInternalAccess" type="SipAccess" />
    <xs:element minOccurs="0" maxOccurs="1" name="SipClientInternalAccess" type="SipAccess" />
    <xs:element minOccurs="0" maxOccurs="1" name="SipServerExternalAccess" type="SipAccess" />
    <xs:element minOccurs="0" maxOccurs="1" name="SipClientExternalAccess" type="SipAccess" />
    <xs:element minOccurs="0" maxOccurs="unbounded" name="link" type="link"/>
  </xs:sequence>
</xs:complexType>
```

## JSON Schema:

```
"User": {
  "id": "User",
  "required": true,
  "type": [
    "object",
    "null"
  ],
},
"properties": {
  "SipServerInternalAccess": {
    "id": "SipAccess",
    "required": true,
    "type": [
      "object",
      "null"
    ],
    "properties": {
      "fqdn": {
        "required": true,
        "type": [
          "string",
          "null"
        ]
      },
      "port": {
        "required": true,
        "type": [
          "string",
          "null"
        ]
      }
    }
  },
  "SipClientInternalAccess": {
    "$ref": "SipAccess"
  },
  "SipServerExternalAccess": {
    "$ref": "SipAccess"
  },
  "SipClientExternalAccess": {
    "$ref": "SipAccess"
  },
  "Links": {
    "$ref": "Link[]"
  }
}
}
```

### 2.2.5 Attributes

The following table summarizes the set of common XML schema attribute definitions defined by this specification. XML schema attributes that are specific to a particular operation are described with the operation.

Attribute	Description
AccessLocation	An indicator of whether the client is connecting from inside or outside of the network.
Fqdn	The <b>fully qualified domain name (FQDN)</b> of the <b>Session Initiation Protocol (SIP)</b> server.
href	A URL that is relative to the service's root URL
Port	The listening port of the SIP server.

Attribute	Description
token	A classification that is used to infer the purpose and use of the attributed item. Somewhat analogous to a type in traditional, compiled programming languages

### 2.2.5.1 AccessLocation

This attribute MUST have values of either "internal" or "external". A value of "internal" indicates that the current server is hosting internal network traffic, while a value of "external" indicates that the current server is hosting external network traffic.

### 2.2.5.2 Fqdn

This attribute specifies the **fully qualified domain name (FQDN)** of the **Session Initiation Protocol (SIP)** server.

### 2.2.5.3 Href

This attribute specifies a URL that is relative to the service's root URL.

### 2.2.5.4 Port

This attribute specifies the listening port of the **SIP** server.

### 2.2.5.5 Token

The following table summarizes the set of possible tokens and their descriptions. For every **token** attribute, there MUST be a corresponding **href** attribute (section [2.2.5.3](#)). The **href** attribute contains a URL that the client can use to access related services. Semantics on the entry points to each URL can be found in the following table. However, no details are provided beyond the entry points.

Token	Description
"Internal/Autodiscover"	Identifies the Autodiscover Service Root entry point that can be accessed from the internal network. See section <a href="#">3.1.5.1</a> for semantics on this URL.
"External/Autodiscover"	Identifies the Autodiscover Service's Root entry point that can be accessed from the external network. See section <a href="#">3.1.5.1</a> for semantics on this URL.
"Internal/AuthBroker"	Identifies the AuthBroker Service entry point that can be accessed from the internal network. This service exposes a SOAP endpoint and publishes a MEX document. The Authbroker Service is specified as the Authentication Broker Service in <a href="#">[MS-OCAUTHWS]</a> . MEX documents are specified in <a href="#">[WS-MetaDataExchange]</a> .
"External/AuthBroker"	Identifies the AuthBroker Service entry point that can be accessed from the external network. This service exposes a SOAP endpoint and publishes a MEX document. The Authbroker Service is specified as the Authentication Broker Service in <a href="#">[MS-OCAUTHWS]</a> . MEX documents are specified in <a href="#">[WS-MetaDataExchange]</a> .
"Internal/Ucwa"	Identifies the Ucwa Service entry point that can be accessed from the internal network. This service exposes a REST endpoint that supports a GET operation. The Ucwa Service is defined in <a href="#">[MS-OCSMP]</a> .
"External/Ucwa"	Identifies the Ucwa Service entry point that can be accessed from the external network. This service exposes a REST endpoint that supports a GET operation. The Ucwa Service is defined in <a href="#">[MS-OCSMP]</a> .



<b>Token</b>	<b>Description</b>
"Redirect"	Identifies an Autodiscover Service URL which is the Root entry point of the next hop in the discovery flow. See section <a href="#">3.1.5.2</a> for semantics on this URL.
"User"	Identifies the Autodiscover Service URL for the User entry point. Semantics on this URL can be found in section <a href="#">3.1.5.3</a> .
"Domain"	Identifies the Autodiscover Service URL for the Domain entry point. Semantics on this URL can be found in section <a href="#">3.1.5.4</a> .
"OAuth"	Identifies the Autodiscover Service URL for the OAuth entry point. Semantics on this URL can be found in section <a href="#">3.1.5.5</a> .

## 3 Protocol Details

### 3.1 Server Details

This section specifies details that pertain to the protocol server behavior.

#### 3.1.1 Abstract Data Model

None.

#### 3.1.2 Timers

None.

#### 3.1.3 Initialization

None.

#### 3.1.4 Higher-Layer Triggered Events

None.

#### 3.1.5 Message Processing Events and Sequencing Rules

The following table lists all the exposed resources by the Autodiscover Service.

Resource	Description
Root	Service entry point that allows navigation to child resources.
User	Provides user home server information.
Domain	Provides general topology information about the current server.
OAuth	Provides user home server information.

##### 3.1.5.1 Common Processing Details

The following table lists all the possible Accept headers handled by the Server, and the Content-Type returned in the response.

Accept Header Values	Returned Content-Type
No Accept header specified	application/vnd.microsoft.rtc.autodiscover+json;v=1
application/vnd.microsoft.rtc.autodiscover+xml;v=1	application/vnd.microsoft.rtc.autodiscover+xml;v=1
Application/vnd.microsoft.rtc.autodiscover+json;v=1	application/vnd.microsoft.rtc.autodiscover+json;v=1
*/*	application/vnd.microsoft.rtc.autodiscover+json;v=1

If none of the Accept headers listed in the table are sent with any request, the server will respond with a 406 (Not Acceptable) response.

If the returned Content-Type is "application/vnd.microsoft.rtc.autodiscover+xml;v=1", then the response will be in XML format and MUST be de-serialized according to the schemas in section [2.2.4](#).

If the returned Content-Type is "application/vnd.microsoft.rtc.autodiscover+json;v=1", then the response will be in **JSON** format and MUST be de-serialized according to the schemas in section [2.2.4](#).

### 3.1.5.2 Root

The Root resource is the entry point to an instance of the Autodiscover Service. All requests to this resource MUST contain the *sipuri* query parameter defined in section [2.2.3.1](#).

The resource URL for this parameter is

`https://<fqdn>/autodiscover/autodiscover.service.svc/root?sipuri=<sipuri>` . The server might also listen on HTTP depending on the server configuration. If a request is made to the HTTP Root resource, the server MUST respond with a **200 OK** and a **Root** element that contains a single **Link** element with token named "Redirect" and an **href** that points to the next hop URL that the client SHOULD request.

If the *sipuri* of the user cannot be processed by the current Autodiscover Service, the Autodiscover Service MUST respond with a 200 OK with a **Root** element that contains a **Link** with a token named "Redirect" and an **href** that points to the next hop URL that can handle the request.

If the current Autodiscover Service can handle the request, then the server MUST respond with a 200 OK and a **Root** element that contains **Link** elements for child resources of the current Autodiscover Service. See section [2.2.4.4](#) for the schema of the **Root** element. If there is no "Redirect" link present in the **Root** element, then there MUST be "User" and "Domain" tokens present. The "OAuth" token might be present depending on the server version.

#### 3.1.5.2.1 GET

This section details the Request and Response body for the supported GET HTTP operation to the Root resource.

##### 3.1.5.2.1.1 Request Body

None.

##### 3.1.5.2.1.2 Response Body

The Autodiscover Service MUST respond with an **AutodiscoverResponse** element (section [2.2.4.1](#)) that contains a **Root** element (section [2.2.4.4](#)).

### 3.1.5.3 User

The User resource exposes **topology** information of a user's home server. The client MUST discover the User URL by parsing the href of the **Link** element in the GET response from the Root resource.

If the request to the User resource does not contain a valid X-Ms-WebTicket header as specified in section [2.2.2.2](#), the server MUST respond with a 401 Unauthorized response.

If a valid X-Ms-WebTicket header is provided and the user's home server information is unknown, the server MUST respond with a 404 Not Found response code and an empty body.

If a valid X-Ms-WebTicket header is provided and the user's home server information exists on a separate server, the server MUST respond with a 200 OK response code and a **User** element. The

**User** element MUST contain only one **Link** element with a "Redirect" Token. Semantics of the "Redirect" Token are defined in [section 2.2.5.5](#).

If a valid X-Ms-WebTicket header is provided and the user's home server information exists on the current server, the server MUST respond with a 200 response code and a **User** element in the body. The **User** element MAY contain any of the following links depending on what is configured in the topology.

1. Internal/Autodiscover
2. External/Autodiscover
3. Internal/AuthBroker
4. External/AuthBroker
5. Internal/Ucwa
6. External/Ucwa

The **SipAccess** types might also be present in the response depending on what is configured in the topology.

### 3.1.5.3.1 GET

This section details the Request and Response body for the supported GET HTTP operation to the User resource.

#### 3.1.5.3.1.1 Request Body

None.

#### 3.1.5.3.1.2 Response Body

If the response code is **200 OK**, then the response MUST contain an **AutodiscoverResponse** element that contains a **User** element. These elements are defined in sections [2.2.4.1](#) and [2.2.4.6](#).

If the response code is 401 Unauthorized, then there will be an **HTML** formatted body.

If the response code is 404 Not Found, then there will be an empty body.

### 3.1.5.4 Domain

The Domain resource exposes information about the topology information of the current server to the client. The client MUST discover the Domain URL by parsing the **Link** element in the GET response from the Root resource.

The Domain resource MUST respond with a **200 OK** to every request and contain a **Domain** element in the body. The **Domain** element is defined in section [2.2.4.2](#).

The **Domain** element MAY contain any of the following links, depending on what is configured in the topology. The links are identified by tokens for which semantics are defined in [section 2.2.5.5](#).

1. Internal/Autodiscover
2. External/Autodiscover
3. Internal/AuthBroker
4. External/AuthBroker

5. Internal/Ucwa
6. External/Ucwa

The **SipAccess** types might also be present in the response, depending on what is configured in the topology.

### 3.1.5.4.1 GET

This section details the Request and Response body for the supported GET HTTP operation to the Domain resource.

#### 3.1.5.4.1.1 Request Body

None.

#### 3.1.5.4.1.2 Response Body

The response MUST contain an **AutodiscoverResponse** element that contains a **Domain** element. These elements are defined in sections [2.2.4.1](#) and [2.2.4.2](#).

### 3.1.5.5 OAuth

The OAuth resource exposes topology information of a user's home server. The client MUST discover the OAuth URL by parsing the href of the **Link** element in the GET response from the Root resource.

If the request to the OAuth resource does not contain an Authorization header as specified in section [2.2.2.1](#), the server MUST respond with a 401 Unauthorized response.

If the request to the OAuth resource contains an invalid Authorization header as specified in section [2.2.2.1](#), the server MUST respond with a 403 Forbidden response.

If a valid Authorization header is provided and the user's home server information is unknown, the server MUST respond with a 404 Not Found response code and an empty body.

If a valid Authorization header is provided and the user's home server information exists on a separate server, the server MUST respond with a **200 OK** response code and a **User** element. The **User** element MUST contain only one link with a "Redirect" token. Semantics of the "Redirect" Token are in section [2.2.5.5](#).

If a valid Authorization header is provided and the user's home server information exists on the current server, the server MUST respond with a 200 response code and a **User** element in the body. The **User** element might contain any of the following links depending on what is configured in the topology.

1. Internal/Autodiscover
2. External/Autodiscover
3. Internal/AuthBroker
4. External/AuthBroker
5. Internal/Ucwa
6. External/Ucwa

The **SipAccess** types might also be present in the response depending on what is configured in the topology

### 3.1.5.5.1 GET

This section details the Request and Response body for the supported GET HTTP operation to the OAuth resource.

#### 3.1.5.5.1.1 Request Body

None.

#### 3.1.5.5.1.2 Response Body

If the response code is **200 OK**, then the response MUST contain an **AutodiscoverResponse** element that contains a **User** element. These elements are defined in sections [2.2.4.1](#) and [2.2.4.6](#).

If the response code is 401 Unauthorized, then there will be an **HTML** formatted body.

If the response code is 404 Not Found, then there will be an empty body.

### 3.1.6 Timer Events

None.

### 3.1.7 Other Local Events

None.

## 3.2 Client Details

This section specifies details that pertain to protocol client behavior.

### 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.

#### 3.2.1.1 Discovery of Autodiscover

The client will usually not have the initial Autodiscover service URL to send the first HTTP request and initiate the protocol flow. The client MUST construct and send requests to as many as four URLs to discover the initial Autodiscover service. The URLs constructed are based off of the client's **Session Initiation Protocol (SIP)** domain and MUST contain the following:

1. `http://lyncdiscoverinternal.<sipdomain>`
2. `https://lyncdiscoverinternal.<sipdomain>`
3. `http://lyncdiscover.<sipdomain>`
4. `https://lyncdiscover.<sipdomain>`

The client MAY execute requests 1 and 2 in parallel, and MAY execute requests 3 and 4 in parallel. The client MUST wait until getting a response from both request 1 and 2 before sending a request to 3 or 4.

The client **MUST** process the result of the first successful request and **MAY** cancel any pending requests after receiving a successful response. The body of the response to any of the previously listed requests **MUST** contain an **AutodiscoverResponse** element which contains a **Root** element.

### 3.2.1.2 Redirect Detection

This protocol will result in many redirects. To prevent any redirect loops, the client **MUST** not allow more than 10 redirects in the entirety of the flow, or the client **MUST** implement redirect loop detection.

### 3.2.1.3 Internal External Network Switching

The final response of the OAuth, User, and Domain resources will contain an **AutodiscoverResponse** element with the **AccessLocation** attribute present, as well as internal and external links of the web services. The internal and external links are both provided in the same response to assist the client in switching between internal and external web services for times when the client is transitioning from inside to outside the network or vice versa. If the **AccessLocation** has the value "internal", the client **SHOULD** use the internal links. If the **AccessLocation** has the value "external", the client **SHOULD** use the external links.

The client also has the ability to probe the Autodiscover service to determine whether it is internal or external without executing the full protocol. After the client obtains the internal and external Autodiscover links, the client **MAY** cache them and probe the Root resource and determine its network location based on the **AccessLocation** value returned in the response. If the client loses network connectivity for a brief period of time, the client **MAY** send a single GET request to the internal and external Autodiscover sites and then connect to the corresponding URL stored in the cache based on the returned **AccessLocation** value.

The client **SHOULD** cache the returned web service URLs until the client receives an error connecting to one of the web services.

### 3.2.2 Timers

None.

### 3.2.3 Initialization

None.

### 3.2.4 Higher-Layer Triggered Events

None.

### 3.2.5 Message Processing Events and Sequencing Rules

None.

### 3.2.6 Timer Events

None.

### 3.2.7 Other Local Events

None.

## 4 Protocol Examples

### 4.1 Discover Home Server

In this scenario, the client follows this protocol to discover its home server URLs.

The client constructs and sends an HTTP and HTTPS request to the Autodiscover service based on its **Session Initiation Protocol (SIP)** URI, john@contoso.com.

```
GET http://lyncdiscover.contoso.com/?sipuri=john@contoso.com HTTP/1.1
Host: contoso.com
Accept: application/vnd.microsoft.rtc.autodiscover+xml;v=1

GET https://lyncdiscoverinternal.contoso.com HTTP/1.1
Host: contoso.com
Accept: application/vnd.microsoft.rtc.autodiscover+xml;v=1
```

The HTTPS request succeeds first with the following result.

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Type: application/vnd.microsoft.rtc.autodiscover+xml;v=1

<?xml version="1.0" encoding="utf-8"?>
<AutodiscoverResponse xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" AccessLocation="Internal">
  <Root>
    <Link token="Domain"
href="https://contoso.com/Autodiscover/AutodiscoverService.svc/root/domain?originalDomain=contoso.com"/>
    <Link token="User"
href="https://contoso.com/Autodiscover/AutodiscoverService.svc/root/user?originalDomain=contoso.com"/>
    <Link token="Self"
href="https://contoso.com/Autodiscover/AutodiscoverService.svc/root?originalDomain=contoso.com"/>
    <Link token="OAuth"
href="https://contoso.com/Autodiscover/AutodiscoverService.svc/root/oauth/user?originalDomain=contoso.com"/>
  </Root>
</AutodiscoverResponse>
```

The client parses the returned links and sends an HTTP GET to the href of the link with the "OAuth" token. The client provides the **JSON** token in the Authorization header.

```
GET https://contoso.com/autodiscover/autodiscover-service.svc/root/oauth/user?originalDomain=contoso.com HTTP/1.1
Host: contoso.com
Authorization: Bearer Y4LBFdjzqXHPxYMHij9snKNWiw0lyShf+i/GU9B+scVnYB3T5BDp6w==
Accept: application/vnd.microsoft.rtc.autodiscover+xml;v=1
```

The server authenticates the client and returns a Redirect response indicating the home server location of the client.

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Type: application/vnd.microsoft.rtc.autodiscover+xml;v=1

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



```
<AutodiscoverResponse xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" AccessLocation="Internal">
  <User>
    <Link href="https://pool1.contoso.com/Autodiscover/AutodiscoverService.svc/root?
originalDomain=contoso.com" token="Redirect"/>
  </User>
</AutodiscoverResponse>
```

The client sends an HTTPS request to redirect the link.

```
GET https://pool1.contoso.com/Autodiscover/AutodiscoverService.svc/root?
originalDomain=contoso.com HTTP/1.1
Host: pool1.contoso.com
Accept: application/vnd.microsoft.rtc.autodiscover+xml;v=1
```

The HTTPS request succeeds with the following result.

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Type: application/vnd.microsoft.rtc.autodiscover+xml;v=1

<?xml version="1.0" encoding="utf-8"?>
<AutodiscoverResponse xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" AccessLocation="Internal">
  <Root>
    <Link token="Domain"
href="https://pool1.contoso.com/Autodiscover/AutodiscoverService.svc/root/domain?
originalDomain=contoso.com"/>
    <Link token="User"
href="https://pool1.contoso.com/Autodiscover/AutodiscoverService.svc/root/user?
originalDomain=contoso.com"/>
    <Link token="OAuth"
href="https://pool1.contoso.com/Autodiscover/AutodiscoverService.svc/root/oauth/user?original
Domain=contoso.com"/>
  </Root>
</AutodiscoverResponse>
```

The client sends an HTTPS request to OAuth link with Authentication header.

```
GET https://pool1.contoso.com/autodiscover/autodiscover-service.svc/root/oauth/user?
originalDomain=contoso.com HTTP/1.1
Host: contoso.com
Authorization: Bearer Y4LBFDjzqXHPxYMHij9snKNWiw0lyShf+i/GU9B+scVnYB3T5BDp6w==
Accept: application/vnd.microsoft.rtc.autodiscover+xml;v=1
```

The HTTPS request succeeds with the following result.

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Type: application/vnd.microsoft.rtc.autodiscover+xml;v=1

<?xml version="1.0" encoding="utf-8"?>
<AutodiscoverResponse AccessLocation="Internal" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <User>
    <Link token="Internal/Autodiscover"
href="https://pool1.contoso.com/Autodiscover/AutodiscoverService.svc/root"/>
    <Link token="Internal/AuthBroker" href="https://pool1.contoso.com/Reach/sip.svc"/>
    <Link token="Internal/Ucwa" href="https://pool1.contoso.com/Ucwa/oauth/v1/applications"/>
  </User>
</AutodiscoverResponse>
```

```
<Link token="External/Autodiscover"
href="https://poollexternal.contoso.com/Autodiscover/AutodiscoverService.svc/root"/>
<Link token="External/AuthBroker"
href="https://poollexternal.contoso.com/Reach/sip.svc"/>
<Link token="External/Ucwa" href="https://poollexternal.contoso.com/Ucwa/
oauth/v1/applications"/>
</User>
</AutodiscoverResponse>
```

## **5 Security**

### **5.1 Security Considerations for Implementers**

None.

### **5.2 Index of Security Parameters**

None.

## 6 Appendix A: Full XML Schema

For ease of implementation, the following is the full XML schema for this protocol.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="AutodiscoverResponse" nillable="true" type="AutodiscoverResponse" />
  <xs:complexType name="AutodiscoverResponse">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="1" name="Root" type="Root" />
      <xs:element minOccurs="0" maxOccurs="1" name="User" type="User" />
      <xs:element minOccurs="0" maxOccurs="1" name="Domain" type="Domain" />
    </xs:sequence>
    <xs:attribute name="AccessLocation" type="xs:string" />
  </xs:complexType>
  <xs:complexType name="Root">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="unbounded" name="Link" type="Link" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="Link">
    <xs:attribute name="token" type="xs:string" />
    <xs:attribute name="href" type="xs:string" />
  </xs:complexType>
  <xs:complexType name="User">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="1" name="SipServerInternalAccess" type="SipAccess" />
      <xs:element minOccurs="0" maxOccurs="1" name="SipClientInternalAccess" type="SipAccess" />
      <xs:element minOccurs="0" maxOccurs="1" name="SipServerExternalAccess" type="SipAccess" />
      <xs:element minOccurs="0" maxOccurs="1" name="SipClientExternalAccess" type="SipAccess" />
      <xs:element minOccurs="0" maxOccurs="unbounded" name="Link" type="Link" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="SipAccess">
    <xs:attribute name="fqdn" type="xs:string" />
    <xs:attribute name="port" type="xs:string" />
  </xs:complexType>
  <xs:complexType name="Domain">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="1" name="SipServerInternalAccess" type="SipAccess" />
      <xs:element minOccurs="0" maxOccurs="1" name="SipClientInternalAccess" type="SipAccess" />
      <xs:element minOccurs="0" maxOccurs="1" name="SipServerExternalAccess" type="SipAccess" />
      <xs:element minOccurs="0" maxOccurs="1" name="SipClientExternalAccess" type="SipAccess" />
      <xs:element minOccurs="0" maxOccurs="unbounded" name="Link" type="Link" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

## 7 Appendix B: Full JSON Schema

For ease of implementation, the following is the full **JSON** schema for this protocol.

```
{
  "id": "AutodiscoverResponse",
  "type": "object",
  "properties": {
    "AccessLocation": {
      "required": true,
      "type": [
        "string",
        "null"
      ]
    },
    "Root": {
      "id": "Root",
      "required": true,
      "type": [
        "object",
        "null"
      ],
      "properties": {
        "Links": {
          "id": "Link[]",
          "required": true,
          "type": [
            "array",
            "null"
          ],
          "items": {
            "id": "Link",
            "type": [
              "object",
              "null"
            ],
            "properties": {
              "token": {
                "required": true,
                "type": [
                  "string",
                  "null"
                ]
              },
              "href": {
                "required": true,
                "type": [
                  "string",
                  "null"
                ]
              }
            }
          }
        }
      }
    },
    "User": {
      "id": "User",
      "required": true,
      "type": [
        "object",
        "null"
      ],
      "properties": {
        "SipServerInternalAccess": {
          "id": "SipAccess",
          "required": true,
          "type": [

```



## 8 Appendix C: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include updates to those products.

- Microsoft Lync Server 2013
- Microsoft Lync Client 2013/Skype for Business
- Microsoft Skype for Business 2016
- Microsoft Skype for Business Server 2015
- Microsoft Skype for Business 2019
- Microsoft Skype for Business Server 2019

Exceptions, if any, are noted in this section. If an update version, service pack or Knowledge Base (KB) number appears with a product name, the behavior changed in that update. The new behavior also applies to subsequent updates unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms "SHOULD" or "SHOULD NOT" implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term "MAY" implies that the product does not follow the prescription.

<1> [Section 2.2.3.1](#): Lync Client 2013/Skype for Business and Lync Server 2013 use the *sipuri* parameter, but the prefix "sip:" is omitted.

## 9 Change Tracking

This section identifies changes that were made to this document since the last release. Changes are classified as Major, Minor, or None.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements.
- A document revision that captures changes to protocol functionality.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **None** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the relevant technical content is identical to the last released version.

The changes made to this document are listed in the following table. For more information, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

Section	Description	Revision class
All	Updated references.	Minor
<a href="#">3.1.5.2</a> Root	Removed instance of a normative term.	Minor
<a href="#">3.1.5.5</a> OAuth	Removed instance of a normative term.	Minor



## 10 Index

### A

Abstract data model:client  
[Data model - abstract:client](#) 22  
Abstract data model:server  
[Data model - abstract:server](#) 18  
[Applicability](#) 7

### C

[Capability negotiation](#) 7  
[Change tracking](#) 32  
Client  
[Abstract data model](#) 22  
[Higher-layer triggered events](#) 23  
[Initialization](#) 23  
[Message processing events and sequencing rules](#) 23  
[Other local events](#) 23  
[Timer events](#) 23  
[Timers](#) 23  
Client:higher-layer triggered events  
[Higher-layer triggered events:client](#) 23  
Client:local events  
[Local events:client](#) 23  
Client:message processing  
[Client:sequencing rules](#) 23  
Client:timer events  
[Timer events:client](#) 23

### D

[Discover Home Server example](#) 24

### E

Examples  
[Discover Home Server](#) 24  
[Discover Home Server example](#) 24

### F

[Fields - vendor-extensible](#) 7  
[Full JSON schema](#) 29  
[Full XML schema](#) 28

### G

[Glossary](#) 5

### H

Headers:custom http  
[Custom HTTP headers](#) 8

### I

[Implementer - security considerations](#) 27  
[Index of security parameters](#) 27  
[Informative references](#) 7  
Initialization:client

[Client:initialization](#) 23  
Initialization:server  
[Server:initialization](#) 18  
[Introduction](#) 5

### J

[JSON schema](#) 29  
[Full JSON schema](#) 29

### M

Messages  
[transport](#) 8  
Messages:attributes  
[Attributes](#) 15  
Messages:complex types  
[Complex types](#) 9  
Messages:namespaces  
[Namespaces](#) 8  
Messages:syntax  
[Syntax:messages - overview](#) 8  
Messages:transport  
[Transport](#) 8

### N

[Namespaces](#) 8  
[Normative references](#) 6

### O

[Overview \(synopsis\)](#) 7

### P

[Parameters - security index](#) 27  
Parameters:common URI  
[Common URI parameters](#) 9  
[Preconditions](#) 7  
[Prerequisites](#) 7  
[Product behavior](#) 31  
Protocol Details  
[Client](#) 22  
[Server](#) 18  
Protocol examples  
[Discover Home Server](#) 24

### R

References  
[informative](#) 7  
[normative](#) 6  
[Relationship to other protocols](#) 7

### S

Security  
[implementer considerations](#) 27  
[parameter index](#) 27  
Server

- [Abstract data model](#) 18
- [Higher-layer triggered events](#) 18
- [Initialization](#) 18
- [Message processing events and sequencing rules](#)  
18
- [Other local events](#) 22
- [Timer events](#) 22
- [Timers](#) 18
- Server:higher-layer triggered events
  - [Higher-layer triggered events:server](#) 18
- Server:local events
  - [Local events:server](#) 22
- Server:message processing
  - [Server:sequencing rules](#) 18
- Server:timer events
  - [Timer events:server](#) 22
- [Standards assignments](#) 7

## **T**

- Timers:client
  - [Client:timers](#) 23
- Timers:server
  - [Server:timers](#) 18
- [Tracking changes](#) 32
- [Transport](#) 8
  - [namespaces](#) 8

## **V**

- [Vendor-extensible fields](#) 7
- [Versioning](#) 7

## **X**

- [XML schema](#) 28
  - [Full XML Schema](#) 28