

[MS-FSADSA]: Active Directory Search Authorization Protocol Specification

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: <http://www.microsoft.com/interop/osp>) or the Community Promise (available here: <http://www.microsoft.com/interop/cp/default.mspx>). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplq@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

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

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

Revision Summary

Date	Revision History	Revision Class	Comments
11/06/2009	0.1	Major	Initial Availability
02/19/2010	1.0	Minor	Updated the technical content
03/31/2010	1.01	Editorial	Revised and edited the technical content

Table of Contents

1	Introduction	5
1.1	Glossary	5
1.2	References.....	5
1.2.1	Normative References.....	5
1.2.2	Informative References	6
1.3	Protocol Overview (Synopsis)	6
1.4	Relationship to Other Protocols.....	7
1.5	Prerequisites/Preconditions	7
1.6	Applicability Statement.....	8
1.7	Versioning and Capability Negotiation.....	8
1.8	Vendor-Extensible Fields.....	8
1.9	Standards Assignments	8
2	Messages.....	9
2.1	Transport.....	9
2.2	Message Syntax	9
2.3	Directory Service Schema Elements	9
3	Protocol Details.....	11
3.1	Client Details.....	11
3.1.1	Abstract Data Model	11
3.1.2	Timers	11
3.1.3	Initialization	11
3.1.4	Higher-Layer Triggered Events.....	11
3.1.5	Message Processing Events and Sequencing Rules.....	11
3.1.5.1	Searching for an Active Directory Object.....	11
3.1.5.2	Reading Active Directory attribute values from an Object.....	12
3.1.6	Timer Events	12
3.1.7	Other Local Events	12
3.2	Server Details	12
3.2.1	Abstract Data Model	12
3.2.2	Timers	12
3.2.3	Initialization	12
3.2.4	Higher-Layer Triggered Events.....	12
3.2.5	Message Processing Events and Sequencing Rules.....	12
3.2.5.1	Searching for an Active Directory Object.....	12
3.2.5.2	Reading Active Directory attribute values from an object	13
3.2.6	Timer Events	13
3.2.7	Other Local Events	13
4	Protocol Examples.....	14
4.1	Example of a search to verify and locate the DN of a user.....	14
4.2	Example that finds the groups that a user belongs to	14
4.3	Example that returns various attributes of a user.....	14
5	Security.....	15
5.1	Security Considerations for Implementers.....	15
5.2	Index of Security Parameters	15
6	Appendix A: Product Behavior.....	16

7 Change Tracking..... 17

8 Index 18

1 Introduction

This document specifies the Active Directory Search Authorization Protocol, which is a subset of the **Lightweight Directory Access Protocol (LDAP)** that accesses the Active Directory. This protocol provides secure search capability, so that user entities receive only the search results for which they are authorized. This protocol also verifies Active Directory user objects and obtains identity information about them, such as group memberships.

1.1 Glossary

The following terms are defined in [\[MS-GLOS\]](#):

directory object
directory service (DS)
distinguished name (DN)
domain controller (DC)
LDAP
Lightweight Directory Access Protocol (LDAP)
object class
Secure Sockets Layer (SSL)
security identifier (SID)

The following terms are defined in [\[MS-OFCGLOS\]](#):

managed property
principal aliasing
principal reference property set
query processing
security principal identifier
user security filter
user store

The following terms are specific to this document:

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

1.2 References

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, <http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624>, as an additional source.

[MS-ADA1] Microsoft Corporation, "[Active Directory Schema Attributes A-L](#)", June 2007.

[MS-ADA2] Microsoft Corporation, "[Active Directory Schema Attributes M](#)", June 2007.

[MS-ADA3] Microsoft Corporation, "[Active Directory Schema Attributes N-Z](#)", June 2007.

[MS-ADLS] Microsoft Corporation, "[Active Directory Lightweight Directory Services Schema](#)", June 2007.

[MS-ADSC] Microsoft Corporation, "[Active Directory Schema Classes](#)", June 2007.

[MS-ADTS] Microsoft Corporation, "[Active Directory Technical Specification](#)", June 2007.

[MS-FSSACFG] Microsoft Corporation, "[Search Authorization Configuration File Format](#)", February 2010.

[MS-OXLDAP] Microsoft Corporation, "[Lightweight Directory Access Protocol \(LDAP\) Version 3 Extensions Specification](#)", June 2008.

[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>

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

[RFC2254] Howes, T., "The String Representation of LDAP Search Filters", RFC 2254, December 1997, <http://www.ietf.org/rfc/rfc2254.txt>

1.2.2 Informative References

[MS-FSQR] Microsoft Corporation, "[Query and Result Protocol Specification](#)", November 2009.

[MS-GLOS] Microsoft Corporation, "[Windows Protocols Master Glossary](#)", March 2007.

[MS-OFCGLOS] Microsoft Corporation, "[Microsoft Office Client Master Glossary](#)", June 2008.

[RFC1777] Yeong, W., Howes, T., and Kille, S., "Lightweight Directory Access Protocol", RFC 1777, March 1995, <http://www.ietf.org/rfc/rfc1777.txt>

[RFC2255] Howes, T., and Smith, M., "The LDAP URL Format", RFC 2255, December 1997, <http://www.ietf.org/rfc/rfc2255.txt>

[RFC3377] Hodges, J., and Morgan, R., "Lightweight Directory Access Protocol (v3): Technical Specification", RFC 3377, September 2002, <http://www.ietf.org/rfc/rfc3377.txt>

[RFC4510] K. Zeilenga, Ed., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", June 2006, <http://www.rfc-editor.org/rfc/rfc4510.txt>

[RFC5246] Dierks, T., and Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008, <http://www.ietf.org/rfc/rfc5246.txt>

1.3 Protocol Overview (Synopsis)

A secure search ensures that user entities receive only the search results for which they are authorized. This occurs in two phases. In the first phase, the customer content repositories are traversed and indexes are created. **Managed properties** that authorize user object access and group object access are added to the indexes for each item.

In the second phase, the user entity is associated with a query, and the protocol client sends that query to the protocol server so that the indexes can quickly identify search results. In this phase, a secure search consists of authenticating the user object and rewriting the query so that the only search results returned are the ones for which the user entity is authorized.

The **query processing** component uses this protocol to obtain the list of groups associated with the specified user object in an Active Directory DS **user store**. The query processing component then modifies the query to apply the **user's security filter**. The user's security filter uses the authorization managed properties to limit the query results to items for which the user entity is authorized, as described in [\[MS-FSQR\]](#) section 3.

Some user objects exist in multiple user stores. For example, an Active Directory DS user object may have a corresponding account under Lotus Notes. To generate the user's security filter, the query processing component needs to be aware of all the names of all associated user entities and associated group objects in all user stores. The **security principal identifier** might not be the same in all user stores. The query processing component handles this with a process called **principal aliasing**, which maps user objects and group objects from one user store to another.

This protocol has three purposes:

1. To verify the existence of user objects and group objects by locating them on the protocol server that is an Active Directory DS **domain controller**.
2. To read the group memberships of an object on the protocol server.
3. To read the values of the attributes of an object on the protocol server. These values include security information for search authorization and for principal aliasing to other user stores.

1.4 Relationship to Other Protocols

This protocol depends on the protocols used by Active Directory for transport, authentication, querying, and reading objects as described in [\[MS-ADTS\]](#). Many of these are based on the Lightweight Directory Access Protocol (LDAP) in [\[RFC1777\]](#), [\[RFC3377\]](#), [\[RFC4510\]](#). **LDAP** is supported directly or over the **Secure Sockets Layer (SSL)** protocol as described in [\[RFC5246\]](#).

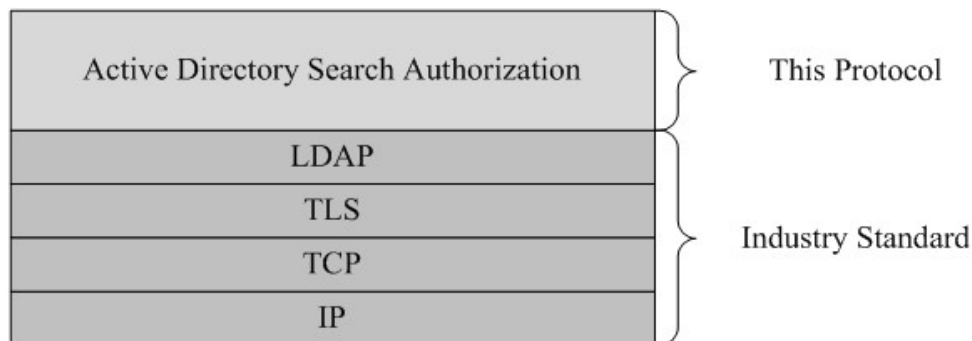


Figure 1: This protocol in relation to other protocols

1.5 Prerequisites/Preconditions

This protocol requires that authentication be performed by the underlying protocols and that the authenticated user entity has sufficient authorization to read the **directory objects** and their attributes.

This protocol uses Simple Authentication as described in [\[MS-ADTS\]](#), section [5.1.1.1.1](#).

The protocol client is required to know the location (URL and port) of the protocol server.

The protocol client is required to know the **distinguished name (DN) (2)** of the Active Directory DS container where it should search for user entities.

The protocol client is required to know the **principal reference property sets** to use for requesting directory object attributes. The principal reference property sets are in the configuration of the user store, as specified in [\[MS-FSSACFG\]](#) section 2.2.

The protocol client is required to know and set necessary underlying protocol configuration options [MS-ADTS], such as referral chasing and timeouts.

1.6 Applicability Statement

This protocol is designed to be used by a query processing component that has been configured with a user store and an Active Directory DS domain controller. This protocol is designed to supply user entity and group entity information to the protocol client from a protocol server that uses limited LDAP.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

This protocol has no Vendor-Extensible fields. However, if all of the following conditions are met, the protocol server MUST return the values of attributes, as specified in [\[MS-ADTS\]](#) section 1.8, when the Active Directory application requests them.

1. A vendor has extended the Active Directory schema with new **object classes** or attributes.
2. Those schema elements are included explicitly in a principal reference property set in the configuration of the protocol client.

1.9 Standards Assignments

There are no standards assignments that have been received explicitly for this protocol. This protocol does make use of the standards assignments that are specified in [\[MS-ADTS\]](#), section [1.9](#).

2 Messages

2.1 Transport

The Active Directory Search Authorization Protocol MUST comply with the transports specified in [\[MS-ADTS\]](#), section [2.1](#).

2.2 Message Syntax

This protocol MUST comply with the message syntaxes specified in [\[MS-ADTS\]](#), section [2.2](#).

2.3 Directory Service Schema Elements

This protocol accesses the **directory service** schema object classes and attributes that are listed in the following table.

Class	Attribute
group	groupType
organizationalPerson1	employeeID givenName initials middleName
person	sn
securityPrincipal	objectSID
top	cn displayName memberOf objectClass samAccountName
user	mailNickname ([MS-OXLDAP] , section 2.2)
Any object class included in a principal reference property set in the configuration of a user store.	Any attribute included in a principal reference property set in the configuration of a user store.

The classes and attributes in the following list are not required for this protocol to operate. They are included in the previous table because they are default values in the principal reference property sets in the configuration of a user store, as specified in [\[MS-FSSACFG\]](#) section 2.2.

- cn
- displayName
- employeeID
- givenName
- group
- groupType

- initials
- mailNickname
- middleName
- organizationalPerson
- person
- sn
- user

For the syntactic specifications of <Class> or <Class><Attribute> pairs, see the following protocols:

- Active Directory Domain Services (ADDS) ([\[MS-ADA1\]](#), [\[MS-ADA2\]](#), [\[MS-ADA3\]](#), [\[MS-ADSC\]](#), and [\[MS-OXLDAP\]](#)).
- Active Directory Lightweight Directory Services (AD/LDS) ([\[MS-ADLS\]](#)).

3 Protocol Details

3.1 Client Details

3.1.1 Abstract Data Model

This protocol uses the abstract data model that is specified in [\[MS-ADTS\]](#), section [3.1.1](#).

The protocol client MUST establish an LDAP connection [\[RFC2251\]](#), section 4.2, which will be used for all protocol requests.

3.1.2 Timers

None.

3.1.3 Initialization

The initialization of this protocol MUST comply with the initialization for a protocol client as specified in [\[MS-ADTS\]](#).

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

All protocol client requests MUST be as specified in [\[MS-ADTS\]](#), section [3](#). Requests are limited to the ones specified in sections [3.1.5.1](#) and [3.1.5.2](#).

3.1.5.1 Searching for an Active Directory Object

The protocol client issues a subtree search request starting from a known node in the Active Directory tree as specified in [\[MS-ADTS\]](#), section [3.1.1.3.1.3](#). The LDAP query MUST be as follows:

```
(|(samAccountName={0}))(objectSID={1}))
```

Replacements are defined in the following table:

Marker	Replacement Value
{0}	The identifier of a user object or group object. This is compared against the Active Directory DS attribute, samAccountName , as specified in [MS-ADA3] .
{1}	The security identifier (SID) of a user or group. This is compared against the Active Directory DS attribute, objectSID , as specified in [MS-ADA3] . The SID is binary and MUST be encoded as specified in [RFC2254] , section 4: each byte will be encoded as a backslash ('\') followed by two hex digits.

The protocol client expects the LDAP query to return a single result that includes the distinguished name (DN).

3.1.5.2 Reading Active Directory attribute values from an Object

The protocol client issues a base search request for a given LDAP object by specifying the LDAP object's distinguished name and a list of attributes the server MUST return if available. The values returned MUST adhere to the values specified in [\[MS-ADTS\]](#), section [3.1.1.2.2.2](#). The list of requested attributes will be **objectSID**, **memberOf**, **objectClass**, **samAccountName** (as specified in [\[MS-ADA2\]](#) and [\[MS-ADA3\]](#)), and all of the attributes in the principal reference property sets.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 Server Details

3.2.1 Abstract Data Model

This protocol MUST have the abstract data model that is specified in [\[MS-ADTS\]](#), section [3.1.1](#).

3.2.2 Timers

This protocol does not explicitly use timers in the protocol server. Timers only exist as specified in [\[MS-ADTS\]](#), section [7.1.6.9.6](#).

3.2.3 Initialization

The protocol server MUST be initialized as specified in [\[MS-ADTS\]](#).

3.2.4 Higher-Layer Triggered Events

All higher-layer triggered events MUST comply with those that are specified in [\[MS-ADTS\]](#).

3.2.5 Message Processing Events and Sequencing Rules

When a request arrives from the protocol client, the protocol server handles it as specified in [\[MS-ADTS\]](#). The only requests that are handled are specified in [3.2.5.1](#) and [3.2.5.2](#).

3.2.5.1 Searching for an Active Directory Object

The protocol server receives a subtree search request starting from a known node in the Active Directory tree as specified in [\[MS-ADTS\]](#), section [3.1.1.3.1.3](#). The LDAP query MUST be as follows:

```
(|(samAccountName={0}))(objectSID={1}))
```

Replacements are defined in the following table:

Marker	Replacement Value
{0}	The identifier of a user object or group object. This is compared against the Active Directory DS attribute, samAccountName , as specified in [MS-ADA3] .

Marker	Replacement Value
{1}	The SID of a user or group. This is compared against the Active Directory DS attribute, objectSID , as specified in [MS-ADA3]. The SID is binary and MUST be encoded as specified in [RFC2254], section 4: each byte will be encoded as a backslash ('\') followed by two hex digits.

The protocol server MUST return either no results or a single result that includes the distinguished name (DN).

3.2.5.2 Reading Active Directory attribute values from an object

The protocol server receives a base search request for a given LDAP object specifying the LDAP object's distinguished name and a list of attributes the server MUST return if available. The values returned MUST adhere to the values specified in [MS-ADTS], section 3.1.1.2.2.2. The list of requested attributes will be **objectSID**, **memberOf**, **objectClass**, **samAccountName** (as specified in [MS-ADA2] and [MS-ADA3]), and all of the attributes in the principal reference property sets.

3.2.6 Timer Events

Timer events MUST comply with those specified in [MS-ADTS].

3.2.7 Other Local Events

All local events MUST comply with those specified in [MS-ADTS].

4 Protocol Examples

These examples are given using the LDAP URL format found in [\[RFC2255\]](#).

4.1 Example of a search to verify and locate the DN of a user

The following example searches for the logon identification of "djones" inside of the "O=Tailspin Toys, C=US" subtree, on the tailspintoys.com server. It also matches a user object whose **objectSID** is the binary value "\11\33\55\77\99\aa\cc\ee".

```
LDAPS://tailspintoys.com:636/O=Tailspin+Toys,C=US??sub?(|(samAccountName=djones)(objectSID=\11\33\55\77\99\aa\cc\ee))
```

4.2 Example that finds the groups that a user belongs to

The following example returns the list of groups of which the user object "CN=David Jones, OU=Users, O=Tailspin Toys, C=US" is a member.

```
LDAPS://tailspintoys.com:636/CN=David+Jones,OU=Users,O=Tailspin+Toys,C=US?memberOf,objectClasses
```

4.3 Example that returns various attributes of a user

The following example returns the values of the attributes **objectClass**, **objectSID** (in binary form), **cn**, **displayName**, **samAccountName**, **sn**, **employeeID**, **givenName**, **initials**, **middleName**, **mailNickname**, and **groupType** (as specified in [\[MS-ADA1\]](#), [\[MS-ADA2\]](#), [\[MS-ADA3\]](#)) for the user object "CN=David Jones, OU=Users, O=Tailspin Toys, C=US".

```
LDAPS://tailspintoys.com:636/CN=David+Jones,OU=Users,O=Tailspin+Toys,C=US?objectClass,objectSID;binary,cn,displayName,samAccountName,sn,employeeID,givenName,initials,middleName,mailNickname,groupType
```

5 Security

5.1 Security Considerations for Implementers

All security for the Active Directory Search Authorization Protocol is described in [\[MS-ADTS\]](#), section [5](#).

This protocol uses Simple Authentication as described in [MS-ADTS], section [5.1.1.1.1](#).

5.2 Index of Security Parameters

The security parameters are handled by the underlying protocol specified in [\[MS-ADTS\]](#), section [5](#).

6 Appendix A: Product Behavior

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

- Microsoft® FAST™ Search Server 2010 for SharePoint®
- Microsoft® FAST™ Search Server 2010 for SharePoint® Internet Sites

Exceptions, if any, are noted below. If a service pack number appears with the product version, behavior changed in that service pack. The new behavior also applies to subsequent service packs of the product unless otherwise specified.

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

7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

8 Index

A

Abstract data model
 [client](#) 11
 [server](#) 12
[Applicability](#) 8

C

[Capability negotiation](#) 8
[Change tracking](#) 17
Client
 [abstract data model](#) 11
 [higher-layer triggered events](#) 11
 [initialization](#) 11
 [message processing](#) 11
 [other local events](#) 12
 [sequencing rules](#) 11
 [timer events](#) 12
 [timers](#) 11
Client – message processing and sequencing rules
 [reading Active Directory attribute values from an object](#) 12
 [searching for an Active Directory object](#) 11

D

Data model - abstract
 [client](#) 11
 [server](#) 12
[Directory service schema elements](#) 9

E

[Elements - directory service schema](#) 9
Examples
 [find the groups that a user belongs to](#) 14
 [overview](#) 14
 [return various attributes of a user](#) 14
 [search to verify and locate the DN of a user](#) 14

F

[Fields - vendor-extensible](#) 8
[Find the groups that a user belongs to - example](#) 14

G

[Glossary](#) 5

H

Higher-layer triggered events
 [client](#) 11
 [server](#) 12

I

[Implementer - security considerations](#) 15

[Index of security parameters](#) 15
[Informative references](#) 6
Initialization
 [client](#) 11
 [server](#) 12
[Introduction](#) 5

M

Message processing
 [client](#) 11
 [server](#) 12
Message processing and sequencing rules – client
 [reading Active Directory attribute values from an object](#) 12
 [searching for an Active Directory object](#) 11
Message processing and sequencing rules – server
 [reading Active Directory attribute values from an object](#) 13
 [searching for an Active Directory object](#) 12
[Message syntax](#) 9
Messages
 [message syntax](#) 9
 [transport](#) 9

N

[Normative references](#) 5

O

Other local events
 [client](#) 12
 [server](#) 13
[Overview \(synopsis\)](#) 6

P

[Parameters - security index](#) 15
[Preconditions](#) 7
[Prerequisites](#) 7
[Product behavior](#) 16

R

References
 [informative](#) 6
 [normative](#) 5
[Relationship to other protocols](#) 7
[Return various attributes of a user - example](#) 14

S

[Schema elements - directory service](#) 9
[Search to verify and locate the DN of a user - example](#) 14
Security
 [implementer considerations](#) 15
 [parameter index](#) 15

- Sequencing rules
 - [client](#) 11
 - [server](#) 12
- Sequencing rules and message processing – client
 - [reading Active Directory attribute values from an object](#) 12
 - [searching for an Active Directory object](#) 11
- Sequencing rules and message processing – server
 - [reading Active Directory attribute values from an object](#) 13
 - [searching for an Active Directory object](#) 12
- Server
 - [abstract data model](#) 12
 - [higher-layer triggered events](#) 12
 - [initialization](#) 12
 - [message processing](#) 12
 - [other local events](#) 13
 - [sequencing rules](#) 12
 - [timer events](#) 13
 - [timers](#) 12
- Server – message processing and sequencing rules
 - [reading Active Directory attribute values from an object](#) 13
 - [searching for an Active Directory object](#) 12
- [Standards assignments](#) 8

T

- Timer events
 - [client](#) 12
 - [server](#) 13
- Timers
 - [client](#) 11
 - [server](#) 12
- [Tracking changes](#) 17
- [Transport](#) 9
- Triggered events - higher-layer
 - [client](#) 11
 - [server](#) 12

V

- [Vendor-extensible fields](#) 8
- [Versioning](#) 8