

# [MS-XWDVSEC]: Web Distributed Authoring and Versioning (WebDAV) Protocol Security Descriptor Extensions

---

## 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 [Open Specification Promise](#) or the [Community Promise](#). 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 [iplg@microsoft.com](mailto:iplg@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. 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, 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
04/04/2008	0.1		Initial Availability.
04/25/2008	0.2		Revised and updated property names and other technical content.
06/27/2008	1.0		Initial Release.
08/06/2008	1.01		Updated references to reflect date of initial release.
09/03/2008	1.02		Updated references.
12/03/2008	1.03		Revised and edited technical content.
03/04/2009	1.04		Revised and edited technical content.
04/10/2009	2.0		Deprecated for Exchange 2010.
07/15/2009	3.0	Major	Changes made for template compliance.
11/04/2009	3.1.0	Minor	Updated the technical content.
02/10/2010	3.2.0	Minor	Updated the technical content.
05/05/2010	3.3.0	Minor	Updated the technical content.
08/04/2010	3.4	Minor	Clarified the meaning of the technical content.
11/03/2010	3.5	Minor	Clarified the meaning of the technical content.
03/18/2011	3.6	Minor	Clarified the meaning of the technical content.
08/05/2011	3.6	No change	No changes to the meaning, language, or formatting of the technical content.
10/07/2011	3.6	No change	No changes to the meaning, language, or formatting of the technical content.
01/20/2012	4.0	Major	Significantly changed the technical content.
04/27/2012	4.0	No change	No changes to the meaning, language, or formatting of the technical content.
07/16/2012	4.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2012	4.1	Minor	Clarified the meaning of the technical content.
02/11/2013	4.1	No change	No changes to the meaning, language, or formatting of the technical content.
07/26/2013	5.0	Major	Significantly changed the technical content.
11/18/2013	5.1	Minor	Clarified the meaning of the technical content.



# Table of Contents

<b>1 Introduction</b>	<b>6</b>
1.1 Glossary	6
1.2 References	6
1.2.1 Normative References	7
1.2.2 Informative References	7
1.3 Overview	8
1.4 Relationship to Other Protocols	8
1.5 Prerequisites/Preconditions	8
1.6 Applicability Statement	8
1.7 Versioning and Capability Negotiation	8
1.8 Vendor-Extensible Fields	8
1.9 Standards Assignments	8
<b>2 Messages</b>	<b>9</b>
2.1 Transport	9
2.2 Message Syntax	9
2.2.1 Namespaces	13
2.2.2 PidTagSecurityDescriptorAsXml Property	13
2.2.3 security_descriptor Element	13
2.2.3.1 from_mapi_tlh Attribute	14
2.2.4 microsoft.security_descriptor Type	14
2.2.5 revision Element	14
2.2.6 owner Element	14
2.2.6.1 defaulted Attribute	14
2.2.7 primary_group Element	15
2.2.7.1 defaulted Attribute	15
2.2.8 dacl Element	15
2.2.8.1 defaulted Attribute	15
2.2.8.2 protected Attribute	15
2.2.8.3 autoinherited Attribute	16
2.2.9 sacl Element	16
2.2.9.1 revision Element	16
2.2.9.2 audit_always Element	16
2.2.9.3 audit_on_failure Element	16
2.2.9.4 audit_on_success Element	17
2.2.9.5 defaulted Attribute	17
2.2.9.6 protected Attribute	17
2.2.9.7 autoinherited Attribute	17
2.2.10 acl Type	18
2.2.10.1 revision Element	18
2.2.10.2 effective_aces Element	18
2.2.10.3 subcontainer_inheritable_aces Element	18
2.2.10.4 subitem_inheritable_aces Element	18
2.2.11 aces Type	19
2.2.11.1 access_allowed_ace Element	19
2.2.11.2 access_denied_ace Element	19
2.2.11.3 system_audit_ace Element	19
2.2.12 inheritable_aces Type	20
2.2.12.1 access_allowed_ace Element	20
2.2.12.2 access_denied_ace Element	20

2.2.12.3	system_audit_ace Element.....	20
2.2.13	ace_T Type.....	20
2.2.13.1	access_mask Element .....	21
2.2.13.2	sid Element.....	21
2.2.13.3	inherited Attribute.....	21
2.2.14	inheritable_ace_T Type .....	21
2.2.14.1	no_propagate_inherit Attribute.....	21
2.2.15	access_mask Element .....	22
2.2.16	sid Type .....	22
2.2.17	NT_Sid Type .....	23
2.2.17.1	string_sid Element .....	23
2.2.17.2	nt4_compatible_name Element.....	24
2.2.17.3	type Element.....	24
2.2.17.4	ad_object_guid Element .....	24
2.2.17.5	display_name Element.....	24
2.2.18	type_string Type .....	24
2.2.19	guid Type .....	25
2.2.20	bool Type .....	25
<b>3</b>	<b>Protocol Details.....</b>	<b>26</b>
3.1	WebDAV Client Details.....	26
3.1.1	Abstract Data Model .....	26
3.1.2	Timers .....	26
3.1.3	Initialization .....	26
3.1.4	Higher-Layer Triggered Events.....	26
3.1.5	Message Processing Events and Sequencing Rules.....	26
3.1.6	Timer Events .....	26
3.1.7	Other Local Events .....	26
3.2	WebDAV Server Details .....	26
3.2.1	Abstract Data Model .....	26
3.2.2	Timers .....	27
3.2.3	Initialization .....	27
3.2.4	Higher-Layer Triggered Events.....	27
3.2.5	Message Processing Events and Sequencing Rules.....	27
3.2.6	Timer Events .....	27
3.2.7	Other Local Events .....	27
<b>4</b>	<b>Protocol Examples.....</b>	<b>28</b>
4.1	Retrieving the Security Descriptor Property .....	28
4.2	Setting the Security Descriptor Property .....	29
<b>5</b>	<b>Security.....</b>	<b>31</b>
5.1	Security Considerations for Implementers.....	31
5.2	Index of Security Parameters .....	31
<b>6</b>	<b>Appendix A: Product Behavior.....</b>	<b>32</b>
<b>7</b>	<b>Change Tracking.....</b>	<b>33</b>
<b>8</b>	<b>Index .....</b>	<b>35</b>

# 1 Introduction

The Web Distributed Authoring and Versioning (WebDAV) Protocol Security Descriptor Extensions extend the **WebDAV** protocol to request and set **security descriptors**. A security descriptor contains security information associated with an entity, such as the entity's owner, which users can access the entity, and so on.

Sections 1.8, 2, and 3 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in RFC 2119. Sections 1.5 and 1.9 are also normative but cannot contain those terms. All other sections and examples in this specification are informative.

## 1.1 Glossary

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

- access control entry (ACE)**
- access control list (ACL)**
- access mask**
- discretionary access control list (DACL)**
- flags**
- GUID**
- Hypertext Transfer Protocol (HTTP)**
- security identifier (SID)**
- user principal name (UPN)**
- XML**
- XML namespace**

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

- mailbox**
- message store**
- Messaging Application Programming Interface (MAPI)**
- permission**
- public folder**
- security descriptor**
- security principal**
- Web Distributed Authoring and Versioning Protocol (WebDAV)**
- WebDAV client**
- WebDAV server**
- XML schema definition (XSD)**

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

References to Microsoft Open Specifications documentation do not include a publishing year because links are to the latest version of the documents, which are updated frequently. References to other documents include a publishing year when one is available.

## 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. 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](#)".
- [MS-ADA3] Microsoft Corporation, "[Active Directory Schema Attributes N-Z](#)".
- [MS-ADTS] Microsoft Corporation, "[Active Directory Technical Specification](#)".
- [MS-DTYP] Microsoft Corporation, "[Windows Data Types](#)".
- [MS-OXCFOLD] Microsoft Corporation, "[Folder Object Protocol](#)".
- [MS-OXPROPS] Microsoft Corporation, "[Exchange Server Protocols Master Property List](#)".
- [MS-SAMR] Microsoft Corporation, "[Security Account Manager \(SAM\) Remote Protocol \(Client-to-Server\)](#)".
- [RFC2068] Fielding, R., Gettys, J., Mogul, J., et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2068, January 1997, <http://www.ietf.org/rfc/rfc2068.txt>
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.rfc-editor.org/rfc/rfc2119.txt>
- [RFC2518] Goland, Y., Whitehead, E., Faizi, A., et al., "HTTP Extensions for Distributed Authoring - WebDAV", RFC 2518, February 1999, <http://www.ietf.org/rfc/rfc2518.txt>
- [W3C-XMLNote] Layman, A., Jung, E., Maler, E., et al., "XML-Data", W3C Note, January 1998, <http://www.w3.org/TR/1998/NOTE-XML-data-0105>
- [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.S., 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.V., 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

- [MS-GLOS] Microsoft Corporation, "[Windows Protocols Master Glossary](#)".
- [MS-OXGLOS] Microsoft Corporation, "[Exchange Server Protocols Master Glossary](#)".
- [MS-OXPROTO] Microsoft Corporation, "[Exchange Server Protocols System Overview](#)".

### 1.3 Overview

As specified in [\[RFC2518\]](#), a **WebDAV client** can retrieve and set properties on a **WebDAV server**. A server can implement a property that represents a security descriptor in **XML**. A client retrieves and sets the security descriptor property on a server by using the WebDAV Protocol Security Extensions. The client can grant or deny access rights to a **security principal** for an entity by adding or removing **access control entries (ACEs)** from the security descriptor's **discretionary access control list (DACL)**.

For example, the client might be an e-commerce application that sells access to research reports. After a customer pays for access to a given report, the application retrieves the security descriptor for the appropriate document, updates it to grant access to the security principal that represents the customer, and sets it on the server. For examples of how a client retrieves and sets the security descriptor, see section [4](#).

### 1.4 Relationship to Other Protocols

The security descriptor property is based on WebDAV, as described in [\[RFC2518\]](#) section 13.

These extensions use the **PROPFIND** and **PROPPATCH** WebDAV methods described in [\[RFC2518\]](#) sections 8.1 and 8.2 to get and set the security descriptor property.

For conceptual background information and overviews of the relationships and interactions between this and other protocols, see [\[MS-OXPROTO\]](#).

### 1.5 Prerequisites/Preconditions

The WebDAV server and WebDAV client applications are required to implement the WebDAV protocol, as specified in [\[RFC2518\]](#), so that the client can set properties on the server.

### 1.6 Applicability Statement

WebDAV clients can use these extensions to get or set the security descriptor for an entity. For example, a client with sufficient **permission** could determine whether to allow various security principals access to a particular entity.

### 1.7 Versioning and Capability Negotiation

This security descriptor property exposes no new versioning capabilities beyond the base protocol of WebDAV and the **Revision** field of the **SECURITY\_DESCRIPTOR** structure, as specified in [\[MS-DTYP\]](#).

### 1.8 Vendor-Extensible Fields

None.

### 1.9 Standards Assignments

There is no standards assignment for this property beyond those assigned for the base WebDAV protocol, as specified in [\[RFC2518\]](#).



## 2 Messages

### 2.1 Transport

Messages are transported by using **HTTP**, as specified in [\[RFC2518\]](#) and [\[RFC2068\]](#).

### 2.2 Message Syntax

The security descriptor property adds to the set of WebDAV properties, as specified in [\[RFC2518\]](#) section 13. The WebDAV Protocol Security Extensions use the **PROPFIND** and **PROPPATCH** WebDAV methods specified in [\[RFC2518\]](#) sections 8.1 and 8.2 to get and set this property. This property is an XML representation of a security descriptor. The type of this property is specified by using **XML schema definition (XSD)** grammar, as specified in [\[XMLSCHEMA1/2\]](#). This property is represented by the **descriptor** XML element, which extends the **security\_descriptor** element defined in the <http://schemas.microsoft.com/security/> **XML namespace**. The XSD for this property is defined as follows.

```
<?xml version="1.0" encoding="utf-8" ?>
<xs:schema xmlns:S="http://schemas.microsoft.com/security/"
  xmlns:D="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/"
  attributeFormDefault="qualified"
  elementFormDefault="qualified"
  targetNamespace="http://schemas.microsoft.com/security/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <!-- Bool is defined to be either 1 or 0 -->
  <xs:simpleType name="bool">
    <xs:restriction base="xs:boolean">
      <xs:pattern value="0|1" />
    </xs:restriction>
  </xs:simpleType>

  <!-- Globally Unique Identifier [MS-DTYP] -->
  <xs:simpleType name="guid">
    <xs:restriction base="xs:string">
      <xs:pattern value="\{[0-9A-Fa-f]{8}-[0-9A-Fa-f]{4}-[0-9A-Fa-f]{4}-[0-9A-
Fa-f]{12}\}" />
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="type_string">
    <xs:restriction base="xs:string">
      <xs:enumeration value="user" />
      <xs:enumeration value="group" />
      <xs:enumeration value="domain" />
      <xs:enumeration value="alias" />
      <xs:enumeration value="well_known_group" />
      <xs:enumeration value="deleted_account" />
      <xs:enumeration value="invalid" />
      <xs:enumeration value="unknown" />
      <xs:enumeration value="computer" />
    </xs:restriction>
  </xs:simpleType>

  <xs:element name="display_name" type="xs:string" />
  <xs:element name="ad_object_guid" type="S:guid" />
  <xs:element name="type" type="S:type_string" />

```

```

<xs:element name="nt4_compatible_name" type="xs:string" />
<xs:element name="string_sid" type="xs:string" />

<xs:complexType name="NT_Sid">
  <xs:sequence>
    <xs:element minOccurs="0" ref="S:string_sid" />
    <xs:element minOccurs="0" ref="S:nt4_compatible_name" />
    <xs:element minOccurs="0" ref="S:type" />
    <xs:element minOccurs="0" ref="S:ad_object_guid" />
    <xs:element minOccurs="0" ref="S:display_name" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="sid">
  <xs:sequence>
    <xs:element name="sid" type="S:NT_Sid" />
  </xs:sequence>
</xs:complexType>

<xs:element name="access_mask">
  <xs:simpleType>
    <xs:restriction base="xs:hexBinary">
      <xs:minLength value="1" />
      <xs:maxLength value="8" />
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<xs:complexType name="ace_T">
  <xs:sequence>
    <xs:element ref="S:access_mask" />
    <xs:element name="sid" type="S:NT_Sid" />
  </xs:sequence>
  <xs:attribute name="inherited" type="S:bool" />
</xs:complexType>

<xs:complexType name="inheritable_ace_T">
  <xs:complexContent mixed="false">
    <xs:extension base="S:ace_T">
      <xs:attribute name="no_propagate_inherit" type="S:bool" />
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="aces">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="unbounded" name="access_allowed_ace"
type="S:ace_T" />
    <xs:element minOccurs="0" maxOccurs="unbounded" name="access_denied_ace" type="S:ace_T"
/>
    <xs:element minOccurs="0" maxOccurs="unbounded" name="system_audit_ace" type="S:ace_T"
/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="inheritable_aces">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="unbounded" name="access_allowed_ace"
type="S:inheritable_ace_T" />
  </xs:sequence>
</xs:complexType>

```

```

        <xs:element minOccurs="0" maxOccurs="unbounded" name="access_denied_ace"
type="S:inheritable_ace_T" />
        <xs:element minOccurs="0" maxOccurs="unbounded" name="system_audit_ace"
type="S:inheritable_ace_T" />
    </xs:sequence>
</xs:complexType>

<xs:element name="revision" type="xs:unsignedInt" />

<xs:complexType name="acl">
    <xs:all minOccurs="0">
        <xs:element ref="S:revision" />
        <xs:element name="effective_aces" type="S:aces" />
        <xs:element name="subcontainer_inheritable_aces" type="S:inheritable_aces" />
        <xs:element name="subitem_inheritable_aces" type="S:inheritable_aces" />
    </xs:all>
</xs:complexType>

<xs:element name="audit_always" type="S:acl" />
<xs:element name="audit_on_failure" type="S:acl" />
<xs:element name="audit_on_success" type="S:acl" />

<xs:element name="sacl">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="S:revision" />
            <xs:element ref="S:audit_always" />
            <xs:element ref="S:audit_on_failure" />
            <xs:element ref="S:audit_on_success" />
        </xs:sequence>
        <xs:attribute name="defaulted" type="S:bool" />
        <xs:attribute name="protected" type="S:bool" />
        <xs:attribute name="autoinherited" type="S:bool" />
    </xs:complexType>
</xs:element>

<xs:element name="dacl">
    <xs:complexType>
        <xs:complexContent mixed="false">
            <xs:extension base="S:acl">
                <xs:attribute name="defaulted" type="S:bool" />
                <xs:attribute name="protected" type="S:bool" />
                <xs:attribute name="autoinherited" type="S:bool" />
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
</xs:element>

<xs:element name="primary_group">
    <xs:complexType>
        <xs:complexContent mixed="false">
            <xs:extension base="S:sid">
                <xs:attribute name="defaulted" type="S:bool" />
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
</xs:element>

<xs:element name="owner">

```

```

<xs:complexType>
  <xs:complexContent mixed="false">
    <xs:extension base="S:sid">
      <xs:attribute name="defaulted" type="S:bool" />
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
</xs:element>

<xs:element name="security_descriptor">
  <xs:complexType>
    <xs:complexContent mixed="false">
      <xs:extension base="D:microsoft.security_descriptor">
        <xs:attribute name="from_mapi_tlh" type="S:bool" />
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
</xs:element>
</xs:schema>

<!-- The base microsoft security descriptor -->
<xs:schema xmlns:S="http://schemas.microsoft.com/security/"
  xmlns:D="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/"
  attributeFormDefault="qualified"
  elementFormDefault="qualified"
  targetNamespace="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:complexType name="microsoft.security_descriptor">
    <xs:all minOccurs="0">
      <xs:element ref="S:revision" />
      <xs:element ref="S:owner" />
      <xs:element ref="S:primary_group" />
      <xs:element ref="S:dacl" />
      <xs:element ref="S:sacl" />
    </xs:all>
  </xs:complexType>
</xs:schema>

<!-- The schema of the actual descriptor property
  This is the property that can be asked for via WebDAV -->

<xs:schema xmlns:S="http://schemas.microsoft.com/security/"
  xmlns:D="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/"
  attributeFormDefault="qualified"
  elementFormDefault="qualified"
  targetNamespace=
    "http://schemas.microsoft.com/exchange/security/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="descriptor">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="S:security_descriptor" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>

```

## 2.2.1 Namespaces

This specification defines and references various XML namespaces by 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	Namespace URI	Reference
S	http://schemas.microsoft.com/security/	
D	urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/	[W3C-XMLNote]
xs	http://www.w3.org/2001/XMLSchema	[XMLSCHEMA1/2]
(none)	http://schemas.microsoft.com/security/	

## 2.2.2 PidTagSecurityDescriptorAsXml Property

Data type: **PtypString**

The **PidTagSecurityDescriptorAsXml** property ([MS-OXPROPS] section 2.987) exposes a security descriptor that represents an entity's security attributes in XML. These attributes specify who owns the entity, who can access it, what they can do with it, what level of audit logging can be applied to the entity, and what kind of restrictions apply to the use of the security descriptor. The security descriptor is a limited XML version of the **SECURITY\_DESCRIPTOR** structure, as specified in [MS-DTYP]. The content of the security descriptor is specified by the **security\_descriptor** element, as specified in section 2.2.3. The schema that specifies the possible values for the **security\_descriptor** element is specified in section 2.2.

Note that the XML security descriptor format does not have a way of transmitting the **SECURITY\_INFORMATION** structure, as specified in [MS-DTYP], which is needed to set the security descriptor on the entity. Instead, the **SECURITY\_INFORMATION** structure is derived from the presence or absence of fields in the XML security descriptor. For example, to set only the DACL on an entity, this property is set with only a DACL in it.

It is possible for a WebDAV client to get this property on an entity when (1) the client created the entity, (2) the client has administrator rights, (3) the entity is in the client's **mailbox**, and (4) the entity is in a **public folder**.

It is possible for a client to set this property on an entity when (1) the client created the entity, (2) the client has administrator rights, (3) the entity is in the client's mailbox, and (4) the entity is in a public folder on which the client has owner permissions.

## 2.2.3 security\_descriptor Element

**Name:** **security\_descriptor**

**Namespace:** http://schemas.microsoft.com/security/

**Type:** **microsoft.security\_descriptor** (section 2.2.4)

**Description:** The **security\_descriptor** element contains the type of the security descriptor specified in section 2.2.2. This element extends the **microsoft.security\_descriptor** type adding a **bool** attribute of **from\_mapi\_tlh**.

### 2.2.3.1 from\_mapi\_tlh Attribute

**Name:** from\_mapi\_tlh

**Namespace:** http://schemas.microsoft.com/security/

**Type:** bool (section [2.2.20](#))

**Description:** The **from\_mapi\_tlh** attribute indicates that the entity for which this security descriptor applies is from a **message store** that is accessible by using WebDAV clients that have the **Messaging Application Programming Interface (MAPI)** enabled.

The absence of this attribute implies that its value is 0. This attribute is applicable only when it is set by the WebDAV server. The WebDAV server MUST ignore this attribute if it is set by a client.

### 2.2.4 microsoft.security\_descriptor Type

**Name:** microsoft.security\_descriptor

**Namespace:** urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/

**Description:** The **microsoft.security\_descriptor** type is the base security descriptor on which the WebDAV server's security descriptor is based.

### 2.2.5 revision Element

**Name:** revision

**Namespace:** http://schemas.microsoft.com/security/

**Type:** unsignedInt, as specified in [\[XMLSCHEMA2/2\]](#) section 3.3.22

**Description:** The **revision** element represents the revision of the **microsoft.security\_descriptor** type, as specified in section [2.2.4](#). If this element is present, its value MUST be set to 1. The absence of this element implies that its value is 1.

### 2.2.6 owner Element

**Name:** owner

**Namespace:** http://schemas.microsoft.com/security/

**Description:** The **owner** element contains the **security identifier (SID)**, as specified in section [2.2.16](#), that specifies the owner of the entity to which the security descriptor is associated. This element can be present. The value of this element is semantically the same as that of the **Owner** member of the **SECURITY\_DESCRIPTOR** structure as specified in [\[MS-DTYP\]](#).

#### 2.2.6.1 defaulted Attribute

**Name:** defaulted

**Namespace:** http://schemas.microsoft.com/security/

**Type:** bool (section [2.2.20](#))

**Description:** The **defaulted** attribute is set when the owner was established by default means. This attribute MUST be present for the **owner** element, as specified in section [2.2.6](#). The value of this

attribute is semantically the same as that specified in [\[MS-DTYP\]](#), relating to the **OD** flag in the **Control** field of the **SECURITY\_DESCRIPTOR** structure.

## 2.2.7 primary\_group Element

**Name:** primary\_group

**Namespace:** <http://schemas.microsoft.com/security/>

**Description:** The **primary\_group** element contains the SID that specifies the group of the entity to which the security descriptor is associated. This element **MUST** be present for the **owner** element, as specified in section [2.2.6](#). The value of this element is semantically the same as that specified for the **Group** member of the **SECURITY\_DESCRIPTOR** structure in [\[MS-DTYP\]](#).

### 2.2.7.1 defaulted Attribute

**Name:** defaulted

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** bool (section [2.2.20](#))

**Description:** The **defaulted** attribute is set when the group was established by default means. This attribute **MUST** be present for the **primary\_group** element, as specified in section [2.2.7](#). The value of this attribute is semantically the same as that specified in [\[MS-DTYP\]](#), relating to the **GD** flag in the **Control** field of the **SECURITY\_DESCRIPTOR** structure.

## 2.2.8 dacl Element

**Name:** dacl

**Namespace:** <http://schemas.microsoft.com/security/>

**Description:** The **dacl** element indicates the DACL. The DACL contains ACEs that grant or deny access to principals or groups. The value of this element is semantically the same as that specified for the **Dacl** member of the **SECURITY\_DESCRIPTOR** structure in [\[MS-DTYP\]](#).

### 2.2.8.1 defaulted Attribute

**Name:** defaulted

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** bool (section [2.2.20](#))

**Description:** The **defaulted** attribute is set when the DACL represented by the **dacl** element, as specified in section [2.2.8](#), was established by default means. This attribute **MUST** be present for the **dacl** element. The value of this attribute is semantically the same as that specified in [\[MS-DTYP\]](#), relating to the **DD** flag in the **Control** field of the **SECURITY\_DESCRIPTOR** structure.

### 2.2.8.2 protected Attribute

**Name:** protected

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** bool (section [2.2.20](#))

**Description:** The **protected** attribute is set when the DACL represented by the **dacl** element, as specified in section [2.2.8](#), SHOULD be protected from inherit operations. This attribute MUST be present for the **dacl** element. The value of this attribute is semantically the same as that specified in [\[MS-DTYP\]](#), relating to the **PD** flag in the **Control** field of the **SECURITY\_DESCRIPTOR** structure.

### 2.2.8.3 autoinherited Attribute

**Name:** autoinherited

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** bool (section [2.2.20](#))

**Description:** The **autoinherited** attribute is set when the **access control list (ACL)** was created through inheritance. This attribute MUST be present for the **dacl** element, as specified in section [2.2.8](#). The value of this attribute is semantically the same as that specified in [\[MS-DTYP\]](#), relating to the **DI** flag in the **Control** field of the **SECURITY\_DESCRIPTOR** structure.

### 2.2.9 sacl Element

**Name:** sacl

**Namespace:** <http://schemas.microsoft.com/security/>

**Description:** The **sacl** element indicates the system **ACL**. This element contains auditing ACEs. The value of this element is semantically the same as that specified for system ACL<1> in [\[MS-DTYP\]](#).

#### 2.2.9.1 revision Element

**Name:** revision

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** unsignedInt, as specified in [\[XMLSCHEMA2/2\]](#) section 3.3.22

**Description:** The **revision** element MUST be present for the **sacl** element, as specified in section [2.2.9](#). This element serves the same purpose as the **AclRevision** field specified in [\[MS-DTYP\]](#) and shares the same appropriate values.

#### 2.2.9.2 audit\_always Element

**Name:** audit\_always

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** acl (section [2.2.10](#))

**Description:** The **audit\_always** element contains the set of ACEs to generate audit messages for access attempts. The value of this element is semantically the same as that specified in [\[MS-DTYP\]](#), relating to the **FAILED\_ACCESS\_ACE\_FLAG** and **SUCCESSFUL\_ACCESS\_ACE\_FLAG** flags.

#### 2.2.9.3 audit\_on\_failure Element

**Name:** audit\_on\_failure

**Namespace:** <http://schemas.microsoft.com/security/>



**Type:** **acl** (section [2.2.10](#))

**Description:** The **audit\_on\_failure** element contains the set of ACEs to generate audit messages for failed access attempts. This element is used in place of the **FAILED\_ACCESS\_ACE\_FLAG** flag of the **AceFlags** field in the **ACE\_HEADER** structure specified in [\[MS-DTYP\]](#) and has the same semantic meaning.

#### 2.2.9.4 audit\_on\_success Element

**Name:** **audit\_on\_success**

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** **acl** (section [2.2.10](#))

**Description:** The **audit\_on\_success** element contains the set of ACEs to generate audit messages for successful access attempts. This element is used in place of the **SUCCESSFUL\_ACCESS\_ACE\_FLAG** flag of the **AceFlags** field in the **ACE\_HEADER** structure specified in [\[MS-DTYP\]](#) and has the same semantic meaning.

#### 2.2.9.5 defaulted Attribute

**Name:** **defaulted**

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** **bool** (section [2.2.20](#))

**Description:** The **defaulted** attribute is set when the system ACL was established by default means. This attribute **MUST** be present for the **sacl** element, as specified in section [2.2.9](#). The value of this attribute is semantically the same as that specified in [\[MS-DTYP\]](#), relating to the **SD** flag in the **Control** field of the **SECURITY\_DESCRIPTOR** structure.

#### 2.2.9.6 protected Attribute

**Name:** **protected**

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** **bool** (section [2.2.20](#))

**Description:** The **protected** attribute is set to protect the system ACL from inherit operations. This attribute **MUST** be present for the **sacl** element, as specified in section [2.2.9](#). The value of this attribute is semantically the same as that specified in [\[MS-DTYP\]](#), relating to the **PS** flag in the **Control** field of the **SECURITY\_DESCRIPTOR** structure.

#### 2.2.9.7 autoinherited Attribute

**Name:** **autoinherited**

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** **bool** (section [2.2.20](#))

**Description:** The **autoinherited** attribute is set when the system ACL was created by inheritance. This attribute **MUST** be present for the **sacl** element, as specified in section [2.2.9](#). The value of this

attribute is semantically the same as that specified in [\[MS-DTYP\]](#), relating to the **SI** flag in the **Control** field of the **SECURITY\_DESCRIPTOR** structure.

### 2.2.10 acl Type

**Name:** **acl**

**Namespace:** <http://schemas.microsoft.com/security/>

**Description:** The **acl** type contains a list of ACEs. This is analogous to the **ACL** type, as specified in [\[MS-DTYP\]](#).

#### 2.2.10.1 revision Element

**Name:** **revision**

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** **unsignedInt**, as specified in [\[XMLSCHEMA2/2\]](#) section 3.3.22

**Description:** The **revision** element indicates the version of the **acl** type, as specified in section [2.2.10](#). This element **MUST** exist. This element serves the same purpose as the **AclRevision** field specified in [\[MS-DTYP\]](#) and shares the same appropriate values.

#### 2.2.10.2 effective\_aces Element

**Name:** **effective\_aces**

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** **aces** (section [2.2.11](#))

**Description:** The **effective\_aces** element contains a list of ACEs that affect the entity. This element can exist if the ACL contains one or more ACEs.

#### 2.2.10.3 subcontainer\_inheritable\_aces Element

**Name:** **subcontainer\_inheritable\_aces**

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** **inheritable\_aces** (section [2.2.12](#))

**Description:** The **subcontainer\_inheritable\_aces** element contains a list of ACEs such that child entities that are containers, such as folders, inherit these ACEs as effective ACEs. This element can exist if the ACL contains one or more ACEs. This is semantically the same as each **ACE** within this element having the **CONTAINER\_INHERIT\_ACE** flag set on the **AceFlags** field of the **ACE\_HEADER** structure, as specified in [\[MS-DTYP\]](#).

#### 2.2.10.4 subitem\_inheritable\_aces Element

**Name:** **subitem\_inheritable\_aces**

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** **inheritable\_aces** (section [2.2.12](#))

**Description:** The **subitem\_inheritable\_aces** element contains a list of ACEs such that noncontainer child entities, such as attachments, inherit these ACEs as effective ACEs. This element can exist if the ACL contains one or more ACEs. This is semantically the same as each ACE within this element having the **OBJECT\_INHERIT\_ACE** flag set on the **AceFlags** field of the **ACE\_HEADER** structure, as specified in [\[MS-DTYP\]](#).

### 2.2.11 aces Type

**Name:** aces

**Namespace:** <http://schemas.microsoft.com/security/>

**Description:** The **aces** type contains a list of non-inheritable ACEs. All the ACEs in this type are semantically the same as the **ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT** flag not being set on an ACE, as specified in [\[MS-DTYP\]](#).

#### 2.2.11.1 access\_allowed\_ace Element

**Name:** access\_allowed\_ace

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** ace\_T (section [2.2.13](#))

**Description:** The **access\_allowed\_aces** element allows access to an entity for a specific trustee identified by a SID. This element can exist if a trustee is allowed access to an entity. This element is only allowed within the **dacl** element, as specified in section [2.2.8](#). This ACE is semantically the same as the **ACCESS\_ALLOWED\_ACE** structure, as specified in [\[MS-DTYP\]](#).

#### 2.2.11.2 access\_denied\_ace Element

**Name:** access\_denied\_ace

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** ace\_T (section [2.2.13](#))

**Description:** The **access\_denied\_ace** element denies access to an entity for a specific trustee identified by a SID. This element can exist if a trustee is denied access to an entity. This element is only allowed within the **dacl** element, as specified in section [2.2.8](#). This ACE is semantically the same as the **ACCESS\_DENIED\_ACE** structure, as specified in [\[MS-DTYP\]](#).

#### 2.2.11.3 system\_audit\_ace Element

**Name:** system\_audit\_ace

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** ace\_T (section [2.2.13](#))

**Description:** The **system\_audit\_ace** element can exist if a trustee is monitored for attempts to access a specific entity. This element is only allowed within the **sacl** element, as specified in section [2.2.10](#). This ACE follows the same semantics as the **SYSTEM\_AUDIT\_ACE** structure, as specified in [\[MS-DTYP\]](#).

## 2.2.12 inheritable\_aces Type

**Name:** inheritable\_aces

**Namespace:** <http://schemas.microsoft.com/security/>

**Description:** The **inheritable\_aces** type contains a list of inheritable ACEs. How these ACEs are inherited is declared by the usage of the **inheritable\_aces** type in either the **subitem\_inheritable\_aces** element, as specified in section [2.2.10.4](#), or the **subcontainer\_inheritable\_aces** element, as specified in section [2.2.10.3](#).

### 2.2.12.1 access\_allowed\_ace Element

**Name:** access\_allowed\_ace

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** inheritable\_ace\_T (section [2.2.14](#))

**Description:** The **access\_allowed\_ace** element allows access to an entity for a specific trustee identified by a SID. This element can exist if a trustee is allowed access to an entity. This element is allowed only within the **dacl** element, as specified in section [2.2.8](#). This ACE is semantically the same as the **ACCESS\_ALLOWED\_ACE** structure, as specified in [\[MS-DTYP\]](#).

### 2.2.12.2 access\_denied\_ace Element

**Name:** access\_denied\_ace

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** inheritable\_ace\_T (section [2.2.14](#))

**Description:** The **access\_denied\_ace** element denies access to an entity for a specific trustee identified by a SID. This element can exist if a trustee is denied access to an entity. This element is only allowed within the **dacl** element, as specified in section [2.2.8](#). This ACE is semantically the same as the **ACCESS\_DENIED\_ACE** structure, as specified in [\[MS-DTYP\]](#).

### 2.2.12.3 system\_audit\_ace Element

**Name:** system\_audit\_ace

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** inheritable\_ace\_T (section [2.2.14](#))

**Description:** The **system\_audit\_ace** element can exist if a trustee is monitored for attempts to access a specific entity. This element is only allowed within the **sacl** element, as specified in section [2.2.10](#). This ACE is semantically the same as the **SYSTEM\_AUDIT\_ACE** structure, as specified in [\[MS-DTYP\]](#).

## 2.2.13 ace\_T Type

**Name:** ace\_T

**Namespace:** <http://schemas.microsoft.com/security/>

**Description:** The **ace\_T** type is the type for ACEs, as specified in section [2.2.11](#).

### 2.2.13.1 access\_mask Element

**Name:** access\_mask

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** access\_mask (section [2.2.15](#))

**Description:** The **access\_mask** element encodes the rights to an entity for a security principal. This element **MUST** exist on all ACEs. The actual **flags** for encoding these rights are specified in section [2.2.15](#).

### 2.2.13.2 sid Element

**Name:** sid

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** NT\_Sid (section [2.2.17](#))

**Description:** The **sid** element identifies a security principal. This element **MUST** exist on all ACEs. This element is semantically the same as the **SID** type, as specified in [\[MS-DTYP\]](#).

### 2.2.13.3 inherited Attribute

**Name:** inherited

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** bool (section [2.2.20](#))

**Description:** The **inherited** attribute indicates that the ACE was inherited. This attribute **MUST** exist. This attribute is semantically the same as the **INHERITED\_ACE** flag in the **AceFlags** field of the **ACE\_HEADER** structure, as specified in [\[MS-DTYP\]](#).

### 2.2.14 inheritable\_ace\_T Type

**Name:** inheritable\_ace\_T

**Namespace:** <http://schemas.microsoft.com/security/>

**Description:** The **inheritable\_ace\_T** type is the base type for all inheritable ACEs. ACEs of this type are the equivalent of having the specific **CONTAINER\_INHERIT\_ACE** or **OBJECT\_INHERIT\_ACE** flags set in the **AceFlags** field of the **ACE\_HEADER** structure as specified in [\[MS-DTYP\]](#).

The **inheritable\_ace\_T** type extends the base **ace\_T** type, as specified in section [2.2.13](#).

#### 2.2.14.1 no\_propagate\_inherit Attribute

**Name:** no\_propagate\_inherit

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** bool (section [2.2.20](#))

**Description:** The **no\_propagate\_inherit** attribute declares that an inherited ACE is not inheritable. This attribute MUST exist. This attribute is semantically the same as the **NO\_PROPAGATE\_INHERIT\_ACE** flag as specified in [MS-DTYP] for the **AceFlags** field flags **CONTAINER\_INHERIT\_ACE** and **OBJECT\_INHERIT\_ACE**.

### 2.2.15 access\_mask Element

**Name:** **access\_mask**

**Namespace:** http://schemas.microsoft.com/security/

**Type:** hexBinary [XMLSCHEMA2/2] section 3.2.15, but limited to between one and eight digits

**Description:** The **access\_mask** element is a 32-bit set of flags that are used to encode the user rights to an entity. An **access mask** is used both to encode the rights to an entity assigned to a security principal and to encode the requested access when opening an entity. This element MUST exist for all ACEs. A bit set to 1 specifies that the allowed or denied right is granted. The unused lower bits MUST be ignored. The lower 16 bits are as follows.

MSB															LSB
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
				V	DOI	WOP	WA	RA		E	WP	RP	AM	WB	RB

Value	Meaning
RB	Read body
WB	Write body
AM	Append message
RP	Read property
WP	Write property
E	Execute
RA	Read attributes
WA	Write attributes
WOP	Write own property
DOI	Delete own item
V	View item

### 2.2.16 sid Type

**Name:** **sid**

**Namespace:** http://schemas.microsoft.com/security/

**Description:** The **sid** type contains the SID that uniquely identifies a security principal. This type wraps an **NT\_Sid** type, as specified in section [2.2.17](#), with a **sid** element.

## 2.2.17 NT\_Sid Type

**Name:** **NT\_Sid**

**Namespace:** <http://schemas.microsoft.com/security/>

**Description:** The **NT\_Sid** type is the XML representation of a SID. It can contain several pieces of information about the security identifier.

If the WebDAV client retrieves the XML representation from the WebDAV server, the following elements will appear in the representation of the **NT\_Sid** type (as long as they are available):

- **string\_sid** (section [2.2.17.1](#))
- **nt4\_compatible\_name** (section [2.2.17.2](#))
- **type** (section [2.2.17.3](#))
- **ad\_object\_guid** (section [2.2.17.4](#))
- **display\_name** (section [2.2.17.5](#))

In some cases, the server returns less information. For example, if the SID cannot be looked up, the server returns only the **string\_sid** element. For some built-in NT accounts, the server returns only the **string\_sid**, **nt4\_compatible\_name**, and **type** elements.

If the WebDAV client sets the XML representation, it does not have to give all the elements, providing that one of the following elements is sufficient:

- **string\_sid**
- **nt4\_compatible\_name**
- **ad\_object\_guid**
- **display\_name**

The server will use only one of the elements that the client gives it to determine the SID. The server SHOULD use the element that is easiest to compute and least prone to ambiguity. The order based on ease of computation is (1) **string\_sid**, (2) **nt4\_compatible\_name**, (3) **ad\_object\_guid**, and (4) **display\_name**. As a last resort, the client can use the **display\_name** element, but because it is not unique, this is not recommended.

### 2.2.17.1 string\_sid Element

**Name:** **string\_sid**

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** **string** [\[XMLSCHEMA2/2\]](#) section 3.2.1

**Description:** The **string\_sid** element identifies a security principal. This element can exist for any SID. This is the string representation of the **SID** type, as specified in [\[MS-DTYP\]](#).

### 2.2.17.2 nt4\_compatible\_name Element

**Name:** nt4\_compatible\_name

**Namespace:** http://schemas.microsoft.com/security/

**Type:** string [\[XMLSCHEMA2/2\]](#) section 3.2.1

**Description:** The **nt4\_compatible\_name** element identifies a security principal. This element can exist for any SID. This element contains a security principal as either a fully qualified account name, such as contoso/someone, or a **user principal name (UPN)**, such as someone@contoso.com.

### 2.2.17.3 type Element

**Name:** type

**Namespace:** http://schemas.microsoft.com/security/

**Type:** type\_string (section [2.2.18](#))

**Description:** The **type** element specifies the type of SID. This element can exist for any SID. The enumeration of values is specified in section [2.2.18](#).

### 2.2.17.4 ad\_object\_guid Element

**Name:** ad\_object\_guid

**Namespace:** http://schemas.microsoft.com/security/

**Type:** guid (section [2.2.19](#)).

**Description:** The **ad\_object\_guid** element identifies a security principal. This element can exist for any SID. The value of this element is a string representation of the **objectGuid** property specified in [\[MS-ADA3\]](#). This property is included so that WebDAV clients that allow users to pick an entry from the directory service, as specified in [\[MS-ADTS\]](#), can specify the entry by giving the **objectGuid** property.

### 2.2.17.5 display\_name Element

**Name:** display\_name

**Namespace:** http://schemas.microsoft.com/security/

**Type:** string [\[XMLSCHEMA2/2\]](#) section 3.2.1

**Description:** The **display\_name** element identifies a security principal. This element can exist for any SID. The value of this element is a display name that WebDAV clients can display in the UI. It comes from the **PidTagDisplayName** property ([\[MS-OXCFOld\]](#) section 2.2.2.2.2.5). It can also be read from the directory service as **displayName**, as specified in [\[MS-ADA1\]](#). Use of this element to identify a security principal is not recommended because the value is not unique.

### 2.2.18 type\_string Type

**Name:** type\_string

**Namespace:** http://schemas.microsoft.com/security/



**Description:** The **type\_string** type specifies the type of SID contained in the **NT\_Sid** type, as specified in section [2.2.17](#). This type can be one of the values listed in the following table.

Value	Meaning
user	A user SID
group	A group SID
domain	A domain SID
alias	An alias SID
well_known_group	A SID for a well-known group
deleted_account	A SID for a deleted account
invalid	A SID that is not valid
unknown	A SID of unknown type
computer	A SID for a computer

These values are semantically the same as those found in the enumeration **SID\_NAME\_USE**, as specified in [\[MS-SAMR\]](#).

### 2.2.19 guid Type

**Name:** **guid**

**Namespace:** <http://schemas.microsoft.com/security/>

**Description:** The **guid** type is a **GUID** that identifies a security principal. This type is semantically the same as the **GUID** structure, as specified in [\[MS-DTYP\]](#). The value of the **guid** type MUST be enclosed by curly braces, for example: "{41a1a32a-4d0f-41ab-ad0c-fb344ef368fd}".

### 2.2.20 bool Type

**Name:** **bool**

**Namespace:** <http://schemas.microsoft.com/security/>

**Type:** **Boolean** [\[XMLSCHEMA2/2\]](#)

**Description:** The **bool** type has the same meaning as specified in [\[XMLSCHEMA2/2\]](#) but is constrained to the values of 0 (zero) and 1.

## 3 Protocol Details

### 3.1 WebDAV Client Details

The security descriptor property that the WebDAV client retrieves from the WebDAV server can contain more information than what is required of the client to set it. Section [2.2.2](#) specifies that the client does not need to set the entire security descriptor to modify the DACL. Additionally, the security descriptor property can contain multiple security principal identifiers for the **NT\_Sid** type, as specified in section [2.2.17](#).

The client can generate all of the security principal identifiers when sending the security descriptor property to the server. It is recommended that the client generate the most precise identifier, as specified in section [2.2.17](#), to avoid ambiguous identifiers.

#### 3.1.1 Abstract Data Model

None.

#### 3.1.2 Timers

None.

#### 3.1.3 Initialization

None.

#### 3.1.4 Higher-Layer Triggered Events

No additional higher-layer triggered events exist beyond those in [\[RFC2518\]](#), and the behavior of any existing higher-layer triggered events is unchanged by this extension.

#### 3.1.5 Message Processing Events and Sequencing Rules

The sequence rules are those that are found for any property, as specified in [\[RFC2518\]](#) section 13.

#### 3.1.6 Timer Events

None.

#### 3.1.7 Other Local Events

None.

### 3.2 WebDAV Server Details

The WebDAV server **MUST** generate all available security principal identifiers when sending the security descriptor property to the WebDAV client. The client can generate all the security principal identifiers when sending the security descriptor property to the server, but the server **MUST** use the most precise identifier that is received from the client, as specified in section [2.2.17](#).

#### 3.2.1 Abstract Data Model

None.

### **3.2.2 Timers**

None.

### **3.2.3 Initialization**

None.

### **3.2.4 Higher-Layer Triggered Events**

No additional higher-layer triggered events exist beyond those specified in [\[RFC2518\]](#), and the behavior of any existing higher-layer triggered events is unchanged by this extension.

### **3.2.5 Message Processing Events and Sequencing Rules**

The sequence rules are those that are found for any property, as specified in [\[RFC2518\]](#) section 13.

### **3.2.6 Timer Events**

None.

### **3.2.7 Other Local Events**

None.

## 4 Protocol Examples

### 4.1 Retrieving the Security Descriptor Property

The security descriptor property can be retrieved using a standard WebDAV **PROPFIND** method request, as specified in [\[RFC2518\]](#), by asking for the **descriptor** element.

For example, the **descriptor** element might look as follows.

```
<d:descriptor xmlns:d="http://schemas.microsoft.com/exchange/security/">
  <S:security_descriptor xmlns:S="http://schemas.microsoft.com/security/"
  xmlns:D="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/" D:dt="microsoft.security_descriptor"
  S:from_mapi_tlh="1">
    <S:revision>1</S:revision>
    <S:owner S:defaulted="0">
      <S:sid>
        <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-1111</S:string_sid>
        <S:type>user</S:type>
        <S:nt4_compatible_name>ELZCHU-DOM\bob</S:nt4_compatible_name>
        <S:ad_object_guid>{138bfc4d-48e0-4d29-9de6-643ecb7314f1}</S:ad_object_guid>
        <S:display_name>bob</S:display_name>
      </S:sid>
    </S:owner>
    <S:primary_group S:defaulted="0">
      <S:sid>
        <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-513</S:string_sid>
        <S:type>group</S:type>
        <S:nt4_compatible_name>ELZCHU-DOM\Domain Users</S:nt4_compatible_name>
        <S:ad_object_guid>{f2a02601-c596-4fd2-9543-d770ba31d9e5}</S:ad_object_guid>
      </S:sid>
    </S:primary_group>
    <S:dacl S:defaulted="1" S:protected="0" S:autoinherited="1">
      <S:revision>2</S:revision>
      <S:effective_aces>
        <S:access_allowed_ace S:inherited="1">
          <S:access_mask>1f0fbf</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-500</S:string_sid>
            <S:type>user</S:type>
            <S:nt4_compatible_name>ELZCHU-DOM\Administrator</S:nt4_compatible_name>
            <S:ad_object_guid>{41a1a32a-4d0f-41ab-ad0c-fb344ef368fd}</S:ad_object_guid>
            <S:display_name>Administrator</S:display_name>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_allowed_ace S:inherited="1">
          <S:access_mask>1f0fbf</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-5-7</S:string_sid>
            <S:type>well_known_group</S:type>
            <S:nt4_compatible_name>NT AUTHORITY\ANONYMOUS LOGON</S:nt4_compatible_name>
            <S:ad_object_guid>{ff158509-ee41-4c44-98c1-affd7edf6a83}</S:ad_object_guid>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_allowed_ace S:inherited="1">
          <S:access_mask>1f0fbf</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-1-0</S:string_sid>
            <S:type>well_known_group</S:type>
```

```

        <S:nt4_compatible_name>\Everyone</S:nt4_compatible_name>
        <S:ad_object_guid>{aa5d6b3e-3546-4f9e-8530-59ad567c6dd8}</S:ad_object_guid>
    </S:sid>
    </S:access_allowed_ace>
</S:effective_aces>
</S:dacl>
</S:security_descriptor>
</d:descriptor>

```

## 4.2 Setting the Security Descriptor Property

To set the security descriptor property by using the **PROPPATCH** method, as specified in [\[RFC2518\]](#), the WebDAV request XML can look like the following.

```

<?xml version='1.0'?>
<d:descriptor xmlns:d='http://schemas.microsoft.com/exchange/security/'>
  <S:security_descriptor xmlns:data='urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/'
  data:dt='microsoft.security_descriptor'>
    <S:dacl xmlns:S='http://schemas.microsoft.com/security/' S:defaulted="0" S:protected="0"
    S:autoinherited="0">
      <S:effective_aces>
        <S:access_allowed_ace>
          <S:access_mask>1f0fbf</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-500</S:string_sid>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_allowed_ace>
          <S:access_mask>1f0fbf</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-5-7</S:string_sid>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_allowed_ace>
          <S:access_mask>1208a9</S:access_mask>
          <S:sid>
            <S:ad_object_guid>{9F4AC28A-2FD0-475E-9736-A9AF92E6612F}</S:ad_object_guid>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_allowed_ace>
          <S:access_mask>1200a9</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-1-0</S:string_sid>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_denied_ace>
          <S:access_mask>d0f16</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-1-0</S:string_sid>
          </S:sid>
        </S:access_denied_ace>
      </S:effective_aces>
      <S:subcontainer_inheritable_aces>
        <S:access_allowed_ace>
          <S:access_mask>1208a9</S:access_mask>
          <S:sid>

```

```
    <S:ad_object_guid>{9F4AC28A-2FD0-475E-9736-A9AF92E6612F}</S:ad_object_guid>
  </S:sid>
</S:access_allowed_ace>
</S:subcontainer_inheritable_aces>
<S:subitem_inheritable_aces>
  <S:access_allowed_ace>
    <S:access_mask>1208a9</S:access_mask>
    <S:sid>
      <S:ad_object_guid>{9F4AC28A-2FD0-475E-9736-A9AF92E6612F}</S:ad_object_guid>
    </S:sid>
  </S:access_allowed_ace>
</S:subitem_inheritable_aces>
</S:dacl>
</S:security_descriptor>
</d:descriptor>
```

## 5 Security

### 5.1 Security Considerations for Implementers

This extension has no security considerations beyond those described in [\[RFC2518\]](#) section 17, [\[RFC2068\]](#) section 15, and [\[MS-DTYP\]](#).

### 5.2 Index of Security Parameters

None.

## 6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product 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 2.2.9:](#) The **sacl** element is not settable in Exchange 2003 and Exchange 2007, but it can appear on items that were upgraded to Exchange 2003 or Exchange 2007.



## 7 Change Tracking

This section identifies changes that were made to the [MS-XWDVSEC] protocol document between the July 2013 and November 2013 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

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 or functionality.
- The removal of a document from the documentation set.

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 **Editorial** means that the formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the technical content of the document is identical to the last released version.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.
- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.

- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated**.

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

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	Tracking number (if applicable) and description	Major change (Y or N)	Change type
<a href="#">2.2.17.2 nt4_compatible_name Element</a>	Revised statement to eliminate the [MS-WPO] reference.	N	Content updated.

## 8 Index

### A

- Abstract data model
  - [client](#) 26
  - [server](#) 26
- access\_allowed\_ace element
  - [aces type](#) 19
  - [inheritable\\_aces type](#) 20
- access\_denied\_ace element
  - [aces type](#) 19
  - [inheritable\\_aces type](#) 20
- [access\\_mask element - ace T type](#) 21
- [access\\_mask Element message](#) 22
- ace\_T type
  - [access\\_mask element](#) 21
  - [inherited attribute](#) 21
  - [sid element](#) 21
- [ace T Type message](#) 20
- aces type
  - [access\\_allowed\\_ace element](#) 19
  - [access\\_denied\\_ace element](#) 19
  - [system\\_audit\\_ace element](#) 19
- [aces Type message](#) 19
- acl type
  - [effective\\_aces element](#) 18
  - [revision element](#) 18
  - [subcontainer\\_inheritable\\_aces element](#) 18
  - [subitem\\_inheritable\\_aces element](#) 18
- [acl Type message](#) 18
- [ad\\_object\\_guid element - NT\\_Sid type](#) 24
- [Applicability](#) 8
- [audit\\_always element - sacl element](#) 16
- [audit\\_on\\_failure element - sacl element](#) 16
- [audit\\_on\\_success element - sacl element](#) 17
- autoinherited attribute
  - [dacl element](#) 16
  - [sacl element](#) 17

### B

- [bool Type message](#) 25

### C

- [Capability negotiation](#) 8
- [Change tracking](#) 33
- Client
  - [abstract data model](#) 26
  - [higher-layer triggered events](#) 26
  - [initialization](#) 26
  - [message processing](#) 26
  - [other local events](#) 26
  - [overview](#) 26
  - [sequencing rules](#) 26
  - [timer events](#) 26
  - [timers](#) 26

### D

- dacl element
  - [autoinherited attribute](#) 16
  - [defaulted attribute](#) 15
  - [protected attribute](#) 15
- [dacl Element message](#) 15
- Data model - abstract
  - [client](#) 26
  - [server](#) 26
- defaulted attribute
  - [dacl element](#) 15
  - [owner element](#) 14
  - [primary\\_group element](#) 15
  - [sacl element](#) 17
- [display\\_name element - NT\\_Sid type](#) 24

### E

- [effective\\_aces element - acl type](#) 18
- Examples
  - [retrieving the security descriptor property](#) 28
  - [setting the security descriptor property](#) 29

### F

- [Fields - vendor-extensible](#) 8
- [from\\_mapi\\_tlh attribute - security\\_descriptor element](#) 14

### G

- [Glossary](#) 6
- [guid Type message](#) 25

### H

- Higher-layer triggered events
  - [client](#) 26
  - [server](#) 27

### I

- [Implementer - security considerations](#) 31
- [Index of security parameters](#) 31
- [Informative references](#) 7
- [inheritable\\_ace T type - no\\_propagate\\_inherit attribute](#) 21
- [inheritable\\_ace T Type message](#) 21
- inheritable\_aces type
  - [access\\_allowed\\_ace element](#) 20
  - [access\\_denied\\_ace element](#) 20
  - [system\\_audit\\_ace element](#) 20
- [inheritable\\_aces Type message](#) 20
- [inherited attribute - ace T type](#) 21
- Initialization
  - [client](#) 26
  - [server](#) 27
- [Introduction](#) 6

## M

### Message processing

[client](#) 26  
[server](#) 27

### Messages

[access\\_mask Element](#) 22  
[ace\\_T Type](#) 20  
[aces Type](#) 19  
[acl Type](#) 18  
[bool Type](#) 25  
[dacl Element](#) 15  
[guid Type](#) 25  
[inheritable\\_ace\\_T Type](#) 21  
[inheritable\\_aces Type](#) 20  
[microsoft.security\\_descriptor Type](#) 14  
[Namespaces](#) 13  
[NT\\_Sid Type](#) 23  
[owner Element](#) 14  
[PidTagSecurityDescriptorAsXml Property](#) 13  
[primary\\_group Element](#) 15  
[revision Element](#) 14  
[sacl Element](#) 16  
[security\\_descriptor Element](#) 13  
[sid Type](#) 22  
[syntax](#) 9  
[transport](#) 9  
[type\\_string Type](#) 24  
[microsoft.security\\_descriptor Type message](#) 14

## N

[Namespaces message](#) 13  
[no\\_propagate\\_inherit attribute - inheritable\\_ace\\_T type](#) 21  
[Normative references](#) 7  
NT\_Sid type  
[ad\\_object\\_guid element](#) 24  
[display\\_name element](#) 24  
[nt4\\_compatible\\_name element](#) 24  
[string\\_sid element](#) 23  
[type element](#) 24  
[NT\\_Sid Type message](#) 23  
[nt4\\_compatible\\_name element - NT\\_Sid type](#) 24

## O

### Other local events

[client](#) 26  
[server](#) 27  
[Overview \(synopsis\)](#) 8  
[owner element - defaulted attribute](#) 14  
[owner Element message](#) 14

## P

[Parameters - security index](#) 31  
[PidTagSecurityDescriptorAsXml Property message](#) 13  
[Preconditions](#) 8  
[Prerequisites](#) 8  
[primary\\_group element - defaulted attribute](#) 15

[primary\\_group Element message](#) 15  
[Product behavior](#) 32  
protected attribute  
[dacl element](#) 15  
[sacl element](#) 17

## R

[References](#) 6  
[informative](#) 7  
[normative](#) 7  
[Relationship to other protocols](#) 8  
[Retrieving the security descriptor property example](#) 28  
revision element  
[acl type](#) 18  
[sacl element](#) 16  
[revision Element message](#) 14

## S

sacl element  
[audit\\_always element](#) 16  
[audit\\_on\\_failure element](#) 16  
[audit\\_on\\_success element](#) 17  
[autoinherited attribute](#) 17  
[default attribute](#) 17  
[protected attribute](#) 17  
[revision element](#) 16  
[sacl Element message](#) 16  
Security  
[implementer considerations](#) 31  
[parameter index](#) 31  
[security\\_descriptor element - from\\_mapi\\_tlh attribute](#) 14  
[security\\_descriptor Element message](#) 13  
Sequencing rules  
[client](#) 26  
[server](#) 27  
Server  
[abstract\\_data\\_model](#) 26  
[higher-layer triggered events](#) 27  
[initialization](#) 27  
[message\\_processing](#) 27  
[other local events](#) 27  
[overview](#) 26  
[sequencing rules](#) 27  
[timer events](#) 27  
[timers](#) 27  
[Setting the security descriptor property example](#) 29  
[sid element - ace\\_T type](#) 21  
[sid Type message](#) 22  
[Standards assignments](#) 8  
[string\\_sid element - NT\\_Sid type](#) 23  
[subcontainer\\_inheritable\\_aces element - acl type](#) 18  
[subitem\\_inheritable\\_aces element - acl type](#) 18  
[Syntax](#) 9  
system\_audit\_ace element  
[aces type](#) 19  
[inheritable\\_aces type](#) 20

## T

Timer events

[client](#) 26

[server](#) 27

Timers

[client](#) 26

[server](#) 27

[Tracking changes](#) 33

[Transport](#) 9

Triggered events - higher-layer

[client](#) 26

[server](#) 27

[type element - NT\\_Sid type](#) 24

[type\\_string\\_Type message](#) 24

## V

[Vendor-extensible fields](#) 8

[Versioning](#) 8