

[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'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
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.

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 Overview	6
1.4 Relationship to Other Protocols	7
1.5 Prerequisites/Preconditions	7
1.6 Applicability Statement	7
1.7 Versioning and Capability Negotiation	7
1.8 Vendor-Extensible Fields	7
1.9 Standards Assignments	7
2 Messages	8
2.1 Transport	8
2.2 Message Syntax	8
2.2.1 Namespaces	12
2.2.2 PidTagSecurityDescriptorAsXml	12
2.2.3 security_descriptor Element	12
2.2.3.1 from_mapi_tlh Attribute	13
2.2.4 microsoft.security_descriptor Type	13
2.2.5 revision Element	13
2.2.6 owner Element	13
2.2.6.1 defaulted Attribute	14
2.2.7 primary_group Element	14
2.2.7.1 defaulted Attribute	14
2.2.8 dacl Element	14
2.2.8.1 defaulted Attribute	14
2.2.8.2 protected Attribute	15
2.2.8.3 autoinherited Attribute	15
2.2.9 sacl Element	15
2.2.9.1 revision Element	15
2.2.9.2 audit_always Element	15
2.2.9.3 audit_on_failure Element	16
2.2.9.4 audit_on_success Element	16
2.2.9.5 defaulted Attribute	16
2.2.9.6 protected Attribute	16
2.2.9.7 autoinherited Attribute	17
2.2.10 acl Type	17
2.2.10.1 revision Element	17
2.2.10.2 effective_aces Element	17
2.2.10.3 subcontainer_inheritable_aces Element	17
2.2.10.4 subitem_inheritable_aces Element	18
2.2.11 aces Type	18
2.2.11.1 access_allowed_ace Element	18
2.2.11.2 access_denied_ace Element	18
2.2.11.3 system_audit_ace Element	19
2.2.12 inheritable_aces Type	19
2.2.12.1 access_allowed_ace Element	19
2.2.12.2 access_denied_ace Element	19

2.2.12.3	system_audit_ace Element.....	19
2.2.13	ace_T Type.....	20
2.2.13.1	access_mask Element	20
2.2.13.2	sid Element.....	20
2.2.13.3	inherited Attribute.....	20
2.2.14	inheritable_ace_T Type	21
2.2.14.1	no_propagate_inherit Attribute.....	21
2.2.15	access_mask Element	21
2.2.16	sid Type	22
2.2.17	NT_Sid Type	22
2.2.17.1	string_sid Element	23
2.2.17.2	nt4_compatible_name Element.....	23
2.2.17.3	type Element.....	23
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
3	Protocol Details.....	26
3.1	Common 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
4	Protocol Examples.....	27
4.1	Retrieving the Property.....	27
4.2	Setting the Property.....	28
5	Security.....	30
5.1	Security Considerations for Implementers.....	30
5.2	Index of Security Parameters	30
6	Appendix A: Product Behavior.....	31
7	Change Tracking.....	32
8	Index	35

1 Introduction

This document specifies an extension to the **WebDAV** protocol, as specified in [\[RFC2518\]](#), by using a standard **HTTP** mechanism specified in [\[RFC2068\]](#). This extension specifies how to request and set the Exchange **security descriptor** by using the WebDAV methods **PROPFIND** and **PROPPATCH**.

1.1 Glossary

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

access control entry (ACE)
access control list (ACL)
Hypertext Transfer Protocol (HTTP)
security descriptor
store
XML
Web Distributed Authoring and Versioning Protocol (WebDAV)
WebDAV client
WebDAV server

The following terms are specific to this document:

discretionary access control list (DACL): An **access control list (ACL)** that is controlled by the owner of an object and that specifies the access particular users or groups can have to that object.

entity: A resource that can be identified by a URL. Use of this term is consistent with that specified in [\[RFC2616\]](#) section 1.3.

property: A named value that is associated with an entity, as specified in [\[RFC2518\]](#) section 13.

security identifier (SID): An identifier for security principals that is used to identify an account or a group. Conceptually, the SID is composed of an account authority portion (typically a domain) and a smaller integer representing an identity relative to the account authority, termed the relative identifier (RID). Use of this term is consistent with that specified in [\[MS-DTYP\]](#).

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", July 2006, <http://go.microsoft.com/fwlink/?LinkId=112308>

- [MS-ADA3] Microsoft Corporation, "Active Directory Schema Attributes N-Z", July 2006, <http://go.microsoft.com/fwlink/?LinkId=112148>
- [MS-ADTS] Microsoft Corporation, "Active Directory Technical Specification", July 2006, <http://go.microsoft.com/fwlink/?LinkId=112149>
- [MS-DTYP] Microsoft Corporation, "Windows Data Types", March 2007, <http://go.microsoft.com/fwlink/?LinkId=111558>
- [MS-NSPI] Microsoft Corporation, "Name Service Provider Interface (NSPI) Protocol Specification", April 2008, <http://go.microsoft.com/fwlink/?LinkId=154742>
- [MS-OXGLOS] Microsoft Corporation, "[Exchange Server Protocols Master Glossary](#)", April 2008.
- [MS-SAMR] Microsoft Corporation, "Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)", July 2006, <http://go.microsoft.com/fwlink/?LinkId=112150>
- [MS-SECO] Microsoft Corporation, "Windows Security Overview", December 2006, <http://go.microsoft.com/fwlink/?LinkId=112307>
- [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", RFC 2119, BCP 14, March 1997, <http://www.ietf.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>
- [RFC2616] Fielding, R., Gettys, J., Mogul, J., et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, <http://www.ietf.org/rfc/rfc2616.txt>
- [W3C-XSD1] Thompson, H., Beech, D., Maloney, M., and Mendelsohn, N., Eds., "XML Schema Part 1: Structures Second Edition", W3C Recommendation, October 2004, <http://www.w3.org/TR/xmlschema-1/>
- [W3C-XSD2] Biron, P., and Malhotra, A., Eds., "XML Schema Part 2: Datatypes Second Edition", W3C Recommendation, October 2004, <http://www.w3.org/TR/xmlschema-2/>
- [XMLNS] Bray, T., Hollander, D., Layman, A., Eds., et al., "Namespaces in XML 1.0 (Third Edition)", December 2009, <http://www.w3.org/TR/REC-xml-names/>

1.2.2 Informative References

- [MSDN-SECNMSPC] Microsoft Corporation, "http://schemas.microsoft.com/exchange/security/ Namespace", November 2001, [http://msdn.microsoft.com/en-us/library/aa566345\(EXCHG.80\).aspx](http://msdn.microsoft.com/en-us/library/aa566345(EXCHG.80).aspx)
- [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>

1.3 Overview

In WebDAV[\[RFC2518\]](#), **properties** can be retrieved and set. A particular property that the server can implement is one that represents a security descriptor, as specified in [\[MS-DTYP\]](#), in **XML**. This property and its type are documented in this specification.

1.4 Relationship to Other Protocols

The descriptor (<http://schemas.microsoft.com/exchange/security/descriptor>) is a property based on WebDAV, as specified in [\[RFC2518\]](#) section 13.

This protocol uses the WebDAV extensions specified in [\[MS-XWDEXT\]](#), specifically in sections [2.2.1.17](#) and [2.2.1.18](#).

1.5 Prerequisites/Preconditions

The server and client applications must implement the WebDAV protocol, as specified in [\[RFC2518\]](#), so that the security descriptor can be set on target items in a database.

1.6 Applicability Statement

This protocol is only useful when a client issuing a WebDAV command requires knowledge of or adjustment to access to an **entity**. For example, a client with sufficient permission could gate access to a particular entity to various security principals.

1.7 Versioning and Capability Negotiation

This security descriptor property exposes no new versioning capabilities beyond the base protocol of WebDAV and the security descriptor revision field, as specified in [\[MS-DTYP\]](#) section 2.4.6.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

There is no standards assignment for this property other than the ones assigned for the base WebDAV protocol [\[RFC2518\]](#).

2 Messages

The security descriptor property adds to the set of WebDAV properties, as specified in [\[RFC2518\]](#) section 13.

2.1 Transport

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

2.2 Message Syntax

This property is an XML representation of a security descriptor. The type of this property is specified by using XSD grammar, as specified in [\[W3C-XSD1\]](#).

```
<?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]
  These MUST be enclosed by curly braces, e.g.
  '{41a1a32a-4d0f-41ab-ad0c-fb344ef368fd}' -->
  <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]{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/	[MSDN-SECNMSPC]
D	urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/	[W3C-XMLNote]
xs	http://www.w3.org/2001/XMLSchema	[W3C-XSD1]
	http://schemas.microsoft.com/security/	[MSDN-SECNMSPC]

2.2.2 PidTagSecurityDescriptorAsXml

Canonical name: [PidTagSecurityDescriptorAsXml](#)

Property name: 0x0E6A

Data type: PtypString, 0x001F

Area: Access Control Properties Property set

Alternate names: <http://schemas.microsoft.com/exchange/security/descriptor>

This property exposes in XML the entity's security attributes. These attributes specify who owns the entity, who can access it and what they can do with it, what level of audit logging can be applied to the object, and what kind of restrictions apply to the use of the security descriptor. This property is a limited XML version of SECURITY_DESCRIPTOR, as specified in [\[MS-DTYP\]](#) section 2.4.6.

One aspect of note in the handling of this property is that the XML security descriptor format does not have a way of transmitting the SECURITY_INFORMATION field needed to set the security descriptor. Instead, the SECURITY_INFORMATION field is derived from the presence/absence of fields in the XML description. So, to set only the **DACL** on an object, this property is set with only a DACL in it.

It is possible for a caller to get this descriptor on an entity when 1) the caller created the object, 2) the caller has administrator rights, 3) the object is in the caller's mailbox, and 4) the object is in a public folder.

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

The content of this property is specified by the <security_descriptor> element, as specified in section [2.2.3](#). The schema that specifies the possible values for this property is specified in section [2.2](#).

2.2.3 security_descriptor Element

Name: security_descriptor

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

Type: **microsoft.security_descriptor** (section [2.2.4](#))

Purpose: This is the type of descriptor specified in section [2.2.2](#)

Description: This type extends the **microsoft.security_descriptor** (section [2.2.4](#)), 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 [3](#))

Purpose: Indicates that the entity for which this security descriptor applies is from a **store** that is accessible via MAPI-enabled clients.

Description: If this attribute is present, the value MUST be 1. Absence of this value implies that its value is 1. This attribute is only applicable when it is set by the server. The 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/>

Purpose: This is the base security descriptor on which the server security descriptor is based.

2.2.5 revision Element

Name: **revision**

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

Type: **unsignedInt**, as specified in [\[W3C-XSD2\]](#) section 3.3.22

Purpose: The revision of the microsoft.security_descriptor type (section 2.2.3).

Description: If 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/>

Purpose: Contains the **SID** (section [2.2.16](#)) that specifies the owner of the entity to which the security descriptor is associated.

Description: This element can be present. This is the same semantics as specified for **Owner** in [\[MS-DTYP\]](#) section 2.4.6.

2.2.6.1 defaulted Attribute

Name: **defaulted**

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

Type: **bool** (section 2.2.19)

Purpose: Set when the owner (section 2.2.5) was established by default means.

Description: This attribute MUST be present for the **owner** element (section 2.2.5). This is the same semantics as specified in [\[MS-DTYP\]](#), section 2.4.6, relating to the Control bit flag OD.

2.2.7 primary_group Element

Name: **primary_group**

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

Purpose: Contains the SID (section [2.2.16](#)) that specifies the group of the entity to which the security descriptor is associated.

Description: This element MUST be present for the **owner** element (section [2.2.6](#)). This is the same semantics as specified for **Group** in [\[MS-DTYP\]](#) section 2.4.6.

2.2.7.1 defaulted Attribute

Name: **defaulted**

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

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

Purpose: Set when the **primary_group** (section [2.2.7](#)) was established by default means.

Description: This attribute MUST be present for the **primary_group** element (section [2.2.7](#)). This is the same semantics as specified in [\[MS-DTYP\]](#) section 2.4.6, relating to the Control bit flag GD.

2.2.8 dacl Element

Name: DACL

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

Purpose: The discretionary **ACL** (section [2.2.10](#)) contains **ACEs** (section [2.2.11](#)) that grant or deny access to principals or groups.

Description: This is the same semantics as specified for DACL in [\[MS-DTYP\]](#) section 2.4.5.

2.2.8.1 defaulted Attribute

Name: **defaulted**

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

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

Purpose: Set when the DACL (section 2.2.7) was established by default means.

Description: This attribute MUST be present for the DACL element (section 2.2.7). This is the same semantics as specified in [\[MS-DTYP\]](#) section 2.4.6, relating to the Control bit flag DD.

2.2.8.2 protected Attribute

Name: protected

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

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

Purpose: Set when the DACL (section 2.2.7) SHOULD be protected from inherit operations.

Description: This attribute MUST be present for the DACL element (section 2.2.7). This is the same semantics as specified in [\[MS-DTYP\]2.4.6](#), relating to the Control bit flag PD.

2.2.8.3 autoinherited Attribute

Name: autoinherited

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

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

Purpose: Set when the ACL (section 2.2.7) was created through inheritance.

Description: This attribute MUST be present for the DACL element (section 2.2.7). This is the same semantics as specified in [\[MS-DTYP\]](#) section 2.4.6, relating to the Control bit flag DI.

2.2.9 sacl Element

Name: **sacl**

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

Purpose: The system ACL (section [2.2.10](#)) contains auditing ACEs (section [2.2.10](#)).

Description: This is the same semantics as specified for system ACL<1> in [\[MS-DTYP\]](#) section 2.4.5.

2.2.9.1 revision Element

Name: **revision**

Namespace: <HTTP://schemas.microsoft.com/security/>

Type: **unsignedInt** as specified in [\[W3C-XSD2\]](#) section 3.3.22

Purpose: This attribute MUST be present for the **sacl** element (section 2.2.8). Serves the same purpose as the **AclRevision** element found 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 2.2.9)

Purpose: The set of ACEs to generate audit messages for access attempts.

Description: This is the same semantic as specified in [\[MS-DTYP\]](#) section 2.4.4.1: AceFlags FAILED_ACCESS_ACE_FLAG and SUCCESSFUL_ACCESS_ACE_FLAG.

2.2.9.3 audit_on_failure Element

Name: **audit_on_failure**

Namespace: HTTP://schemas.microsoft.com/security/

Type: ACL (section 2.2.9)

Purpose: The set of ACEs to generate audit messages for failed access attempts.

Description: This is used in place of [\[MS-DTYP\]](#) AceFlag FAILED_ACCESS_ACE_FLAG 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](#))

Purpose: The set of ACEs to generate audit messages for successful access attempts.

Description: This is used in place of [\[MS-DTYP\]](#) section [2.4.6](#) AceFlag SUCCESSFUL_ACCESS_ACE_FLAG 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](#))

Purpose: Set when the system ACL (section 2.2.8) was established by default means.

Description: This attribute **MUST** be present for the **sacl** element (section 2.2.8). This is the same semantics as specified in [\[MS-DTYP\]](#), relating to the Control bit flag SD.

2.2.9.6 protected Attribute

Name: protected

Namespace: HTTP://schemas.microsoft.com/security/

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

Purpose: Set when the system ACL (section [2.2.10](#)) should be protected from inherit operations.

Description: This attribute **MUST** be present for the <sacl> element (section [2.2.9](#)). This is the same semantics as specified in [\[MS-DTYP\]](#) section 2.4.6, relating to the Control bit flag PS.

2.2.9.7 autoinherited Attribute

Name: autoinherited

Namespace: HTTP://schemas.microsoft.com/security/

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

Purpose: Set when the system ACL (section 2.2.8) was created by inheritance.

Description: This attribute **MUST** be present for the **sacl** element (section 2.2.8). This is the same semantics as specified in [\[MS-DTYP\]](#) section 2.4.6, relating to the Control bit flag SI.

2.2.10 acl Type

Name: ACL

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

Purpose: **Access control list**

Description: Contains a list of ACEs. This is analogous to ACL, as specified in [\[MS-DTYP\]](#) section 2.4.5.

2.2.10.1 revision Element

Name: **revision**

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

Type: **unsignedInt**, as specified in [\[W3C-XSD2\]](#) section 3.3.22

Purpose: Indicates the version of the ACL Type (section [2.2.10](#)).

Description: This element **MUST** exist. Serves the same purpose as the **AclRevision** element found in [\[MS-DTYP\]](#) section 2.4.5 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](#))

Purpose: This element can exist if the ACL contains one or more ACEs. Contains a list of ACEs that affect the entity of which **descriptor** ([2.2.2](#)) is a property.

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](#))

Purpose: Contains a list of ACEs such that child objects that are containers, such as folders, inherit these ACEs as effective ACEs (section [2.2.10.2](#)).

Description: This element can exist if the ACL contains one or more ACEs. Semantically the same as having each ACE within here having the CONTAINER_INHERIT_ACE flag set on the **AceFlags** as defined in [\[MS-DTYP\]](#) section 2.4.4.1.

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](#))

Purpose: Contains a list of ACEs such that non-container child objects, such as attachments, inherit these ACEs as effective ACEs (section [2.2.10.2.](#))

Description: This element can exist if the ACL contains one or more ACEs. Semantically the same as having each ACE within here having the OBJECT_INHERIT_ACE flag set on **AceFlags**, as specified in [\[MS-DTYP\]](#) section 2.4.4.1.

2.2.11 aces Type

Name: ACEs

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

Purpose: Contains a list of non-inheritable ACEs (section [2.2.11.1](#) through [2.2.11.3](#))

Description: All the ACEs in this type are semantically the same as having the flag ACE_INHERITED_OBJECT_TYPE_PRESENT not set, as specified in [\[MS-DTYP\]](#) section 2.4.4.3.

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](#))

Purpose: Allows access to an entity for a specific trustee identified by a SID (section [2.2.18](#)).

Description: This ACE is only allowed on DACLs (section [2.2.8](#)). This element can exist if a trustee is allowed access to an entity. This ACE follows the same semantics as **ACCESS_ALLOWED_ACE**, as specified in [\[MS-DTYP\]](#) section 2.4.4.2.

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](#))

Purpose: Denies access to an entity for a specific trustee identified by a SID (section [2.2.18](#)).

Description: This ACE is allowed only on DACLs (section [2.2.8](#)). This element can exist if a trustee is denied access to an entity. This ACE follows the same semantics as **ACCESS_DENIED_ACE**, as specified in [\[MS-DTYP\]](#) section 2.4.4.4.

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](#))

Purpose: System-audit ACE.

Description: This ACE is only allowed on system ACLs (section [2.2.9](#)). This element can exist if a trustee is monitored for attempts to access a specific object. This ACE follows the same semantics as **SYSTEM_AUDIT_ACE**, as specified in [\[MS-DTYP\]](#) section 2.4.4.9.

2.2.12 inheritable_aces Type

Name: **inheritable_aces**

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

Purpose: Contains a list of inheritable ACEs.

Description: How these ACEs are inherited is declared by the usage of this type in either **subitem_inheritable_aces** (section [2.2.10.4](#)) or **subcontainer_inheritable_aces** (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](#))

Purpose: Allows access to an entity for a specific trustee identified by a **SID** (section [2.2.16](#)).

Description: This element can exist if a trustee is allowed access to an entity. This ACE is only allowed on DACLs (section [2.2.8](#)). This ACE follows the same semantics as **ACCESS_ALLOWED_ACE**, as specified in [\[MS-DTYP\]](#) section 2.4.4.2.

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](#))

Purpose: Denies access to an entity for a specific trustee identified by a SID (section [2.2.16](#)).

Description: This element can exist if a trustee is denied access to an entity. This ACE is only allowed on DACLs (section [2.2.8](#)). This ACE follows the same semantics as **ACCESS_DENIED_ACE**, as specified in [\[MS-DTYP\]](#) section 2.4.4.4.

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](#))

Purpose: System-audit ACE.

Description: This element can exist if a trustee is monitored for attempts to access a specific object. This ACE is only allowed on system ACLs (section [2.2.9](#)). This ACE follows the same semantics as **SYSTEM_AUDIT_ACE**, as specified in [\[MS-DTYP\]](#) section 2.4.4.9.

2.2.13 ace_T Type

Name: **ace_T**

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

Purpose: The base type for ACEs.

Description: The type for access control entries found in ACEs (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](#))

Purpose: Encodes the rights to an entity for a security principal.

Description: 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](#))

Purpose: Identifies a security principal.

Description: This element **MUST** exist on all ACEs. Semantically the same as SID, as specified in [\[MS-DTYP\]](#) section 2.4.2.

2.2.13.3 inherited Attribute

Name: **inherited**

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

Type: **bool** (section [2.2.19](#))

Purpose: Indicates that the ACE was inherited.

Description: This attribute **MUST** exist. Semantically the same as the **AceFlags INHERITED_ACE**, as specified in [\[MS-DTYP\]](#) section 2.4.4.1.

2.2.14 inheritable_ace_T Type

Name: **inheritable_ace_T**

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

Purpose: The base type for all inheritable ACEs (section [2.2.12](#)).

Description: ACEs of this type are the equivalent of having the specific **AceFlags** **CONTAINER_INHERIT_ACE** or **OBJECT_INHERIT_ACE** set as specified in [\[MS-DTYP\]](#) section 2.4.4.1.

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](#))

Purpose: Declares that an inherited ACE is not inheritable.

Description: This attribute **MUST** exist. This is semantically the same as **NO_PROPAGATE_INHERIT_ACE** as found in [\[MS-DTYP\]](#) section 2.4.4.1 for the **AceFlags** **CONTAINER_INHERIT_ACE** and **OBJECT_INHERIT_ACE**.

2.2.15 access_mask Element

Name: **access_mask**

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

Type: **hexBinary** [\[W3C-XSD2\]](#) section 3.2.15, but limited to between one and eight digits.

Purpose: 32-bit set of flags that are used to encode the user rights to an object. An access mask is used both to encode the rights to an object assigned to a principal and to encode the requested access when opening an object.

Description: 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	Description
RB	Read Body
WB	Write Body

Value	Description
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/>

Purpose: Contains the security identifier (SID) that uniquely identifies a security principal.

Description: This specific type simply wraps an **NT_Sid** (section [2.2.17](#)) with a "<sid>" element.

2.2.17 NT_Sid Type

Name: **NT_Sid**

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

Purpose: Contains a security identifier (SID).

Description: It is important to understand more about the XML representation of NT security identifiers. Note that it can be seen that a number of different pieces of information about the security identity are available.

If you retrieve from the **WebDAV server** the XML representation, all the following elements will appear in the representation of the **NT_Sid** (as long as they are available):

<string_sid> (see section [2.2.17.1](#))

<nt4_compatible_name> (see section [2.2.17.2](#))

<type> (see section [2.2.17.3](#))

<ad_object_guid> (see section [2.2.17.4](#))

<display_name> (see section [2.2.17.5](#))

In some cases, less information is returned. For example, if the SID cannot be looked up, you would see only the string SID. For some built-in NT accounts, you will only get the **string_sid**, **nt4_compatible_name**, and **type**.

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> (see section [2.2.17.1](#))

<nt4_compatible_name> (see section [2.2.17.2](#))

<ad_object_guid> (see section [2.2.17.4](#))

<display_name>(see section [2.2.17.5](#))

The WebDAV server will only use one of the elements that the WebDAV client gives it to determine the SID. The WebDAV 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 **display_name**, but because of the ambiguity problems, this would probably not be a good choice.

2.2.17.1 string_sid Element

Name: **string_sid**

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

Type: **string** [[W3C-XSD2](#)] section 3.2.1.

Purpose: Identifies a security principal.

Description: This element can exist for any SID (section [2.2.16](#)). This is the string representation of the SID as specified in [\[MS-DTYP\]](#) section 2.4.2.

2.2.17.2 nt4_compatible_name Element

Name: **nt4_compatible_name**

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

Type: **string** [[W3C-XSD2](#)] section 3.2.1

Purpose: Identifies a security principal.

Description: This element can exist for any SID (section [2.2.16](#)). Contains a security principal as either a fully qualified account name (domain_name/user_name) or a user principal name (user_name@domain_name) as specified in [\[MS-SECO\]](#) section 2.2.

2.2.17.3 type Element

Name: **type**

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

Type: **type_string** (section [2.2.18](#))

Purpose: Value that specifies the type of SID.

Description: This element can exist for any SID (section [2.2.16](#)). 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](#))

Purpose: Identifies a security principal.

Description: This element can exist for any SID (section [2.2.16](#)). The value of this is a string representation of the **objectGuid** property specified in [\[MS-ADA3\]](#) section 2.43. This property is included so clients that allow users to pick an entry from the directory service [\[MS-ADTS\]](#) 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** [\[W3C-XSD2\]](#) section 3.2.1.

Purpose: Identifies a security principal.

Description: This element can exist for any SID (section [2.2.16](#)). The value of this is a display name that clients can display in the UI. It comes from the [PidTagDisplayName](#) property, as specified in [\[MS-OXPROPS\]](#) section 2.749. It can also be read from the directory service as displayName [\[MS-ADA1\]](#) section [2.175](#). The downside of identifying a security principal by using this element is that it is not unique.

2.2.18 type_string Type

Name: **type_string**

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

Purpose: Specifies the possible type of **NT_SID** (section [2.2.17](#)).

Description: Can be one of the following values:

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.

Value	Meaning
computer	A SID for a computer.

These values are semantically the same as those found in the enumeration **SID_NAME_USE**, as defined in [\[MS-SAMR\]](#) section 2.2.2.3.

2.2.19 guid Type

Name: **GUID**

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

Purpose: Globally unique identifier.

Description: Used to identify a security principal. Semantically the same as [\[MS-DTYP\]](#) section 2.3.2.

2.2.20 bool Type

Name: **bool**

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

Type: **Boolean** [\[W3C-XSD2\]](#) section 3.2.2

Purpose: To indicate a **Boolean** state.

Description: This has the same meaning as specified in [\[W3C-XSD2\]](#) section 3.2.2, but is constrained to the values of 0 (zero) and 1.

3 Protocol Details

3.1 Common Details

The **descriptor** property that is retrieved from the 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 (section [2.2.8](#)). Additionally, the **descriptor** property can contain multiple security principal identifiers for the NT_Sid type (section [2.2.17](#)). The server MUST generate all available security principal identifiers when the property is sent to the client. Clients can generate all the security identifiers but the server MUST use the most precise identifier that is received from the client, as specified in section [2.2.17](#). It is recommended that the client generate the most precise security principal identifier, as specified in section [2.2.17](#), to avoid ambiguous identifiers.

3.1.1 Abstract Data Model

No additional data is required beyond that specified in [\[RFC2518\]](#).

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.

4 Protocol Examples

This section gives examples of how to retrieve and set this property.

4.1 Retrieving the Property

This security descriptor can be retrieved via a standard WebDAV **PROPFIND** request by asking for the property:

`http://schemas.microsoft.com/exchange/security/descriptor`

For example, the property **descriptor** 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>lf0fbf</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>lf0fbf</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:effective_aces>
    </S:dacl>
  </S:security_descriptor>
</d:descriptor>
```

```

        </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 Property

To set a security descriptor by using the PROPPATCH method, the WebDAV request XML can look like this:

```

<?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 property has no security considerations beyond those specified in [\[RFC2518\]](#) section 17, [\[RFC2616\]](#) section 15, and [\[MS-DTYP\]](#) section 4.

5.2 Index of Security Parameters

None.

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® Office Outlook® 2003
- Microsoft® Exchange Server 2003
- Microsoft® Office Outlook® 2007
- Microsoft® Exchange Server 2007

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.

[<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 from earlier systems.

7 Change Tracking

This section identifies changes made to [MS-XWDVSEC] protocol documentation between February 2010 and May 2010 releases. Changes are classed as major, minor, or editorial.

Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- An extensive rewrite, addition, or deletion of major portions of content.
- A protocol is deprecated.
- The removal of a document from the documentation set.
- Changes made for template compliance.

Minor changes do not affect protocol interoperability or implementation. Examples are updates to fix technical accuracy or ambiguity at the sentence, paragraph, or table level.

Editorial changes apply to grammatical, formatting, and style issues.

No changes means that the document is identical to its last release.

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

- New content added.
- Content update.
- 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.
- New content added for template compliance.
- Content updated for template compliance.

- Content removed for template compliance.
- Obsolete document removed.

Editorial changes always have the revision type "Editorially updated."

Some important terms used in revision 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.

Changes are listed in the following table. If you need further information, please contact protocol@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
1.1 Glossary	51978 Updated the section reference in the glossary definition for "entity".	N	Content update.
1.1 Glossary	51975 Updated the definition for "security identifier (SID)".	N	Content update.
1.2.1 Normative References	Added [XMLNS] reference information.	N	Content update.
1.2.2 Informative References	Added reference information for [MSDN-SECNMSC].	N	Content update.
1.3 Overview	Updated the section title.	N	Content updated for template compliance.
1.4 Relationship to Other Protocols	51972 Added information about dependencies on WebDAV extensions.	N	New content added.
1.6 Applicability Statement	51996 Changed the term "property" to "protocol".	N	Content update.
2 Messages	51995 Clarified that the property referenced is the security identifier property.	N	Content update.
2.2.1 Namespaces	Added new section.	N	New content added.
2.2.2 PidTagSecurityDescriptorAsXml	51999 Added information about what	N	Content update.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
	content is used to set the value for this property.		
2.2.2 PidTagSecurityDescriptorAsXml	51997 Removed normative language that indicated optional behavior.	N	Content update.
2.2.4 microsoft.security_descriptor Type	52008 Removed information about an analogous structure.	N	Content removed.
2.2.9 sacl Element	51973 Removed a reference to the Exchange 2010 product.	N	Product behavior note updated.
2.2.10.1 revision Element	51977 Updated the reference to point to the correct XML schema specification document.	N	Content update.
2.2.13.2 sid Element	52006 Updated the sid element type information.	N	Content update.
2.2.15 access_mask Element	54804 Added a table header row.	N	Content updated for template compliance.
2.2.15 access_mask Element	52000 Removed behavior information.	N	Content removed.
2.2.17 NT_Sid Type	52002 Clarified the order in which security identifier elements are used.	N	Content update.
3.1 Common Details	52003 Updated the section title.	N	Content updated for template compliance.
3.1.5 Message Processing Events and Sequencing Rules	52004 Removed the statement that the client sends a WebDAV command to retrieve or set the property value.	N	Content updated for template compliance.
4.1 Retrieving the Property	52001 Moved information about setting the property to section 4.2.	N	Content removed.
4.2 Setting the Property	52001 Added a new section for setting the property.	N	New content added.

8 Index

A

Abstract data model
[client](#) 26
[Applicability](#) 7

C

[Capability negotiation](#) 7
[Change tracking](#) 32
Client
[abstract data model](#) 26
[higher-layer triggered events](#) 26
[message processing](#) 26
[sequencing rules](#) 26

D

Data model – abstract
[client](#) 26

E

[Examples - overview](#) 27

G

[Glossary](#) 5

H

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

I

[Implementer - security considerations](#) 30
[Introduction](#) 5

M

Message processing
[client](#) 26
Messages
[overview](#) 8
[transport](#) 8

N

[Normative references](#) 5

O

[Overview](#) 6

P

[Preconditions](#) 7

[Prerequisites](#) 7
[Product behavior](#) 31

R

References
[normative](#) 5
[Relationship to other protocols](#) 7

S

Security
[implementer considerations](#) 30
[overview](#) 30
Sequencing rules
[client](#) 26
[Standards assignments](#) 7

T

[Tracking changes](#) 32
Triggered events - higher-layer
[client](#) 26

V

[Versioning](#) 7