

# [MS-XWDVSEC]: WebDAV Extensions for Security Protocol Specification

## Intellectual Property Rights Notice for Protocol Documentation

- **Copyrights.** This protocol 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 protocols, and may distribute portions of it in your implementations of the protocols 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 protocol documentation.
- **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 protocols. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, the protocols may be covered by Microsoft's Open Specification Promise (available here: <http://www.microsoft.com/interop/osp>). If you would prefer a written license, or if the protocols are not covered by the OSP, patent licenses are available by contacting [protocol@microsoft.com](mailto:protocol@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.

**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.** This protocol documentation is 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. A protocol specification does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them.

Revision Summary			
Author	Date	Version	Comments
Microsoft Corporation	April 4, 2008	0.1	Initial Availability.
Microsoft Corporation	April 25, 2008	0.2	Revised and updated property names and other technical content.
Microsoft Corporation	June 27, 2008	1.0	Initial Release.
Microsoft Corporation	August 6, 2008	1.01	Updated references to reflect date of initial release.
Microsoft Corporation	September 3, 2008	1.02	Updated references.
Microsoft Corporation	December 3, 2008	1.03	Revised and edited technical content.

Revision Summary			
Author	Date	Version	Comments
Microsoft Corporation	March 4, 2009	1.04	Revised and edited technical content.

# Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>5</b>
1.1	Glossary .....	5
1.2	References .....	6
1.2.1	Normative References .....	6
1.2.2	Informative References .....	6
1.3	Protocol 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
<b>2</b>	<b>Messages.....</b>	<b>7</b>
2.1	Transport.....	7
2.2	Message Syntax.....	7
2.2.1	PidTagSecurityDescriptorAsXml.....	12
2.2.2	security_descriptor Element.....	12
2.2.2.1	from_mapi_tlh Attribute .....	12
2.2.3	microsoft.security_descriptor Type .....	13
2.2.4	revision Element.....	13
2.2.5	owner Element.....	13
2.2.5.1	defaulted Attribute.....	13
2.2.6	primary_group Element .....	13
2.2.6.1	defaulted Attribute.....	13
2.2.7	dacl Element .....	14
2.2.7.1	defaulted Attribute.....	14
2.2.7.2	protected Attribute.....	14
2.2.7.3	autoinherited Attribute .....	14
2.2.8	sacl Element.....	15
2.2.8.1	revision Element .....	15
2.2.8.2	audit_always Element .....	15
2.2.8.3	audit_on_failure Element.....	15
2.2.8.4	audit_on_success Element .....	15
2.2.8.5	defaulted Attribute.....	15
2.2.8.6	protected Attribute.....	16
2.2.8.7	autoinherited Attribute .....	16
2.2.9	acl Type.....	16
2.2.9.1	revision Element.....	16
2.2.9.2	effective_aces Element.....	16
2.2.9.3	subcontainer_inheritable_aces Element .....	17
2.2.9.4	subitem_inheritable_aces Element .....	17
2.2.10	aces Type .....	17

2.2.10.1	access_allowed_ace Element.....	17
2.2.10.2	access_denied_ace Element.....	17
2.2.10.3	system_audit_ace Element.....	18
2.2.11	inheritable_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.....	18
2.2.12	ace_T Type .....	19
2.2.12.1	access_mask Element.....	19
2.2.12.2	sid Element .....	19
2.2.12.3	inherited Attribute.....	19
2.2.13	inheritable_ace_T Type.....	19
2.2.13.1	no_propagate_inherit Attribute.....	20
2.2.14	access_mask Element.....	20
2.2.15	sid Type.....	21
2.2.16	NT_Sid Type .....	21
2.2.16.1	string_sid Element.....	22
2.2.16.2	nt4_compatible_name Element .....	22
2.2.16.3	type Element .....	22
2.2.16.4	ad_object_guid Element.....	22
2.2.16.5	display_name Element .....	22
2.2.17	type_string Type.....	23
2.2.18	guid Type.....	23
2.2.19	bool Type.....	23
<b>3</b>	<b>Protocol Details.....</b>	<b>24</b>
3.1	Client/Server Details .....	24
3.1.1	Abstract Data Model .....	24
3.1.2	Timers .....	24
3.1.3	Initialization.....	24
3.1.4	Higher-Layer Triggered Events.....	24
3.1.5	Message Processing Events and Sequencing Rules .....	24
3.1.6	Timer Events.....	24
3.1.7	Other Local Events.....	24
<b>4</b>	<b>Protocol Examples.....</b>	<b>25</b>
4.1	Retrieving the Property .....	25
<b>5</b>	<b>Security.....</b>	<b>27</b>
5.1	Security Considerations for Implementers.....	27
5.2	Index of Security Parameters.....	27
<b>6</b>	<b>Appendix A: Office/Exchange Behavior.....</b>	<b>28</b>
	<b>Index.....</b>	<b>29</b>

# 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 identifier (SID)**  
**property**  
**store**  
**XML**

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 2.3.

**security descriptor:** The **SECURITY\_DESCRIPTOR** structure that defines an entity's security. It specifies the security principal that owns the entity, the security principal(s) that can access the entity and what they can do with it, what level of audit logging has to be applied to the entity, and what type of restrictions apply to the use of the security descriptor. For more information, see [MS-DTYP] section 2.4.6.

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

**Web Distributed Authoring and Versioning Protocol (WebDAV):** The protocol specified in [RFC2518].

**WebDAV client:** A computer that uses the **WebDAV** protocol, as specified in [RFC2518], to retrieve data from the **WebDAV server**.

**WebDAV server:** A computer that supports the **WebDAV protocol**, as specified in [RFC2518], to and from which **WebDAV clients** can connect and retrieve data.

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

## **1.2 References**

### **1.2.1 Normative References**

- [MS-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", June 2008.
- [MS-OXGLOS] Microsoft Corporation, "Exchange Server Protocols Master Glossary", June 2008.
- [MS-SAMR] Microsoft Corporation, "Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)", <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., 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.ietf.org/rfc/rfc2119.txt>.
- [RFC2518] Goland Y., et al., "HTTP Extensions for Distributed Authoring – WEBDAV", RFC 2518, February 1999, <http://www.ietf.org/rfc/rfc2518.txt>.
- [RFC2616] Fielding, R., et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, <http://www.ietf.org/rfc/rfc2616.txt>.
- [W3C-XSD1] World Wide Web Consortium, "XML Schema Part 1: Structures Second Edition", October 2004, <http://www.w3.org/TR/xmlschema-1/>.
- [W3C-XSD2] World Wide Web Consortium, "XML Schema Part 2: Datatypes Second Edition", October 2004, <http://www.w3.org/TR/xmlschema-2/>.

### **1.2.2 Informative References**

None.

## **1.3 Protocol 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. Its value is that of a security descriptor that controls access to an entity.

## ***1.5 Prerequisites/Preconditions***

For this **property** to be exposed, a **WebDAV** method to retrieve or set is operated against an entity on which this property exists.

## ***1.6 Applicability Statement***

This **property** 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**

This **property** adds to the set of 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: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:all>
</xs:complexType>

```

```

        <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: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 PidTagSecurityDescriptorAsXml

**Canonical name:** PidNameCalendarResources

**Property set:**

**Property name:** 0x0E6A

**Data type:** PtypString, 0x001F

**Area:** Common

**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 SHOULD 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.

Also, it is not possible to get this descriptor on an entity and set it back on the entity unless the caller also created the object. When the caller resets the security descriptor, the XML representation includes the owner, and the **store** (and **NT**) will not allow a normal user to set the owner of an object to anyone other than that user.

### 2.2.2 security\_descriptor Element

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

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

**Type:** **microsoft.security\_descriptor** (section 2.2.3)

**Purpose:** This is the type of descriptor specified in section 2.2.1.

**Description:** This type extends the **microsoft.security\_descriptor** (section 2.2.3), adding a **bool** attribute of **from\_mapi\_tlh**.

#### 2.2.2.1 from\_mapi\_tlh Attribute

**Name:** **from\_mapi\_tlh**

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

**Type:** **bool** (section 2.2.19)

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

**Description:** This value MAY be present. If present, it MUST be "1" ". Absence of this value implies that its value is "1".

### 2.2.3 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. It was designed to be analogous to the **SECURITY\_DESCRIPTOR** structure ([MS-DTYP] section 2.4.6) and shares nearly all of the same field names.

### 2.2.4 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: This field MAY be present. If present, its value MUST be set to "1". The absence of this element implies that its value is "1".

### 2.2.5 owner Element

Name: **owner**  
Namespace: http://schemas.microsoft.com/security/  
Purpose: Contains the **SID** (section 2.2.15) that specifies the owner of the entity to which the **security\_descriptor** is associated.  
Description: This element MAY be present. This is the same semantics as specified for **Owner** in [MS-DTYP] section 2.4.6.

#### 2.2.5.1 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.

### 2.2.6 primary\_group Element

Name: **primary\_group**  
Namespace: http://schemas.microsoft.com/security/  
Purpose: Contains the **SID** (section 2.2.15) 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 2.2.5). This is the same semantics as specified for **Group** in [MS-DTYP] section 2.4.6.

#### 2.2.6.1 defaulted Attribute

Name: **defaulted**  
Namespace: http://schemas.microsoft.com/security/  
Type: **bool** (section 2.2.17)

**Purpose:** Set when the **primary\_group** (section 2.2.6) was established by default means.

**Description:** This attribute **MUST** be present for the **primary\_group** element (section 2.2.6). This is the same semantics as specified in [MS-DTYP] section 2.4.6, relating to the Control bit flag GD.

### 2.2.7 dacl Element

**Name:** **dacl**

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

**Purpose:** The discretionary **ACL** (section 2.2.9) contains **ACEs** (section 2.2.10) 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.

#### 2.2.7.1 defaulted Attribute

**Name:** **defaulted**

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

**Type:** **bool** (section 2.2.17)

**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.

#### 2.2.7.2 protected Attribute

**Name:** **protected**

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

**Type:** **bool** (section 2.2.17)

**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] section 2.4.6, relating to the Control bit flag PD.

#### 2.2.7.3 autoinherited Attribute

**Name:** **autoinherited**

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

**Type:** **bool** (section 2.2.17)

**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.

### 2.2.8 sacl Element

Name: **sac1**  
Namespace: <http://schemas.microsoft.com/security/>  
Purpose: The system **ACL** (section 2.2.9) contains auditing **ACEs** (section 2.2.10).  
Description: This is the same semantics as specified for system ACL in [MS-DTYP] section 2.4.5.

#### 2.2.8.1 revision Element

Name: **revision**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **unsignedInt** as specified in [W3C-XSD2] section 3.3.22  
Purpose: This attribute MAY be present for the **sac1** element (section 2.2.8). Serves the same purpose as the **AclRevision** element found in [MS-DTYP] section 2.4.5 and shares the same appropriate values.

#### 2.2.8.2 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.

#### 2.2.8.3 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] section 2.4.4.1 AceFlag FAILED\_ACCESS\_ACE\_FLAG and has the same semantic meaning.

#### 2.2.8.4 audit\_on\_success Element

Name: **audit\_on\_success**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **acl** (section 2.2.9)  
Purpose: The set of **ACEs** to generate audit messages for successful access attempts.  
Description: This is used in place of [MS-DTYP] section 2.4.4.1 AceFlag SUCCESSFUL\_ACCESS\_ACE\_FLAG and has the same semantic meaning.

#### 2.2.8.5 defaulted Attribute

Name: **defaulted**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **bool** (section 2.2.17)

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] section 2.4.6, relating to the Control bit flag SD.

### 2.2.8.6 protected Attribute

Name: **protected**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **bool** (section 2.2.17)  
Purpose: Set when the system **ACL** (section 2.2.8) should be protected from inherit operations.  
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 PS.

### 2.2.8.7 autoinherited Attribute

Name: **autoinherited**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **bool** (section 2.2.17)  
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.

### 2.2.9 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.

#### 2.2.9.1 revision Element

Name: **revision**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **unsignedInt**, as specified in [W3C-XSD] section 3.3.22  
Purpose: Indicates the version of the **ACL** Type (section 2.2.9).  
Description: This element **MAY** exist. Serves the same purpose as the **AclRevision** element found in [MS-DTYP] section 2.4.5 and shares the same appropriate values.

#### 2.2.9.2 effective\_aces Element

Name: **effective\_aces**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **aces** (section 2.2.10)  
Purpose: This element **MAY** exist. Contains a list of **ACEs** that affect the entity of which **descriptor** (section 2.2.1) is a property.



### 2.2.9.3 subcontainer\_inheritable\_aces Element

Name: **subcontainer\_inheritable\_aces**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **inheritable\_aces** (section 2.2.11)  
Purpose: Contains a list of **ACEs** such that child objects that are containers, such as folders, inherit these ACEs as effective ACEs (section 2.2.9.2).  
Description: This element MAY exist. 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.

### 2.2.9.4 subitem\_inheritable\_aces Element

Name: **subitem\_inheritable\_aces**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **inheritable\_aces** (section 2.2.11)  
Purpose: Contains a list of **ACEs** such that non-container child objects, such as attachments, inherit these ACEs as effective ACEs (section 2.2.9.2).  
Description: This element MAY exist. Semantically the same as having each ace within here having the OBJECT\_INHERIT\_ACE flag set on them as specified in [MS-DTYP] section 2.4.4.1.

### 2.2.10 aces Type

Name: **aces**  
Namespace: <http://schemas.microsoft.com/security/>  
Purpose: Contains a list of non-inheritable **ACES** (section 2.2.10.1 through 2.2.10.6)  
Description: All the ACEs in this type are semantically the same as having the flag ACE\_INHERITED\_OBJECT\_TYPE not set as specified in [MS-DTYP] section 2.4.4.2.

#### 2.2.10.1 access\_allowed\_ace Element

Name: **access\_allowed\_ace**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **ace\_T** (section 2.2.12)  
Purpose: Allows access to an entity for a specific trustee identified by a **SID** (section 2.2.17).  
Description: This **ACE** is only allowed on **DACLs** (section 2.2.7). This element MAY exist. This ACE follows the same semantics as **ACCESS\_ALLOWED\_ACE**, as specified in [MS-DTYP] section 2.4.4.2.

#### 2.2.10.2 access\_denied\_ace Element

Name: **access\_denied\_ace**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **ace\_T** (section 2.2.12)  
Purpose: Denies access to an entity for a specific trustee identified by a **SID** (section 2.2.17).

Description: This **ACE** is allowed only on **DACLs** (section 2.2.7). This element MAY exist. This ACE follows the same semantics as **ACCESS\_DENIED\_ACE**, as specified in [MS-DTYP] section 2.4.4.4.

### 2.2.10.3 **system\_audit\_ace** Element

Name: **system\_audit\_ace**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **ace\_T** (section 2.2.12)  
Purpose: System-audit ace.  
Description: This **ACE** is only allowed on system **ACLs** (section 2.2.8). This element MAY exist. This ACE follows the same semantics as **SYSTEM\_AUDIT\_ACE**, as specified in [MS-DTYP] section 2.4.4.9.

### 2.2.11 **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 2.2.9.4) or **subcontainer\_inheritable\_aces** (section 2.2.9.3).

#### 2.2.11.1 **access\_allowed\_ace** Element

Name: **access\_allowed\_ace**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **inheritable\_ace\_T** (section 2.2.15)  
Purpose: Allows access to an entity for a specific trustee identified by a **SID** (section 2.2.17).  
Description: This element MAY exist. This **ACE** is only allowed on **DACLs** (section 2.2.7). 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: **inheritable\_ace\_T** (section 2.2.13)  
Purpose: Denies access to an entity for a specific trustee identified by a **SID** (section 2.2.17).  
Description: This element MAY exist. This **ACE** is only allowed on **DACLs** (section 2.2.7). 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: **inheritable\_ace\_T** (section 2.2.15)  
Purpose: System-audit ace.  
Description: This element MAY exist. This **ACE** is only allowed on system **ACLs** (section 2.2.8). This ACE follows the same semantics as **SYSTEM\_AUDIT\_ACE**, as specified in [MS-DTYP] section 2.4.4.9.

### 2.2.12 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 2.2.10).

#### 2.2.12.1 access\_mask Element

Name: **access\_mask**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **access\_mask** (section 2.2.14)  
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 2.2.14.

#### 2.2.12.2 sid Element

Name: **sid**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **sid** (section 2.2.15)  
Purpose: Identifies a security principal.  
Description: This element MUST exist on all **ACEs**. Semantically the same as **SID** as specified in section 2.4.4 [MS-DTYP].

#### 2.2.12.3 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.

### 2.2.13 inheritable\_ace\_T Type

Name: **inheritable\_ace\_T**  
Namespace: <http://schemas.microsoft.com/security/>  
Purpose: The base type for all inheritable **ACEs** (section 2.2.11)

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.

### 2.2.13.1 no\_propagate\_inherit Attribute

Name: **no\_propagate\_inherit**  
 Namespace: <http://schemas.microsoft.com/security/>  
 Type: **bool** (section 2.2.17)  
 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 section 2.4.4.1 [MS-DTYP] for the **AceFlags** **CONTAINER\_INHERIT\_ACE** and **OBJECT\_INHERIT\_ACE**.

### 2.2.14 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. Clients **MUST** use the same definition of the top 16 bits that Windows does in [MS-DTYP] section 2.4.3. 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
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

### 2.2.15 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 2.2.18) with a "<sid>" element.

### 2.2.16 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 2.2.18.1)
<nt4_compatible_name>	(see section 2.2.18.2)
<type>	(see section 2.2.18.3)
<ad_object_guid>	(see section 2.2.18.4)
<display_name>	(see section 2.2.18.5)

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 2.2.18.1)
<nt4_compatible_name>	(see section 2.2.18.2)
<ad_object_guid>	(see section 2.2.18.4)
<display_name>	(see section 2.2.18.5)

The WebDAV server will only use one of the elements the WebDAV client gives it to determine the SID. It SHOULD pick the cheapest element to work from. The notion of cost of determining which SID the client means is according to the order of the previous list – so use **string\_sid** if it is known, else **nt4\_compatible\_name**, and so on. As a last resort the client MAY use **display\_name**, but because of the ambiguity problems, this would probably not be a good choice.

### 2.2.16.1 **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 MAY exist for any **SID** (section 2.2.15). This is the string representation of the SID as specified in section 2.4.2 [MS-DTYP].

### 2.2.16.2 **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 MAY exist for any **SID** (section 2.2.15). 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.

### 2.2.16.3 **type** Element

Name: **type**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **type\_string** (section 2.2.17)  
Purpose: Value that specifies the type of **SID**.  
Description: This element MAY exist for any **SID** (section 2.2.15). The enumeration of values is specified in section 2.2.19.

### 2.2.16.4 **ad\_object\_guid** Element

Name: **ad\_object\_guid**  
Namespace: <http://schemas.microsoft.com/security/>  
Type: **guid** (section 2.2.18)  
Purpose: Identifies a security principal.  
Description: This element MAY exist for any **SID** (section 2.2.15). 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-OLABK] can specify the entry by giving the **objectGuid** property.

### 2.2.16.5 **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 MAY exist for any **SID** (section 2.2.15). 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-NSPI]. 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.

### 2.2.17 type\_string Type

Name: **type\_string**

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

Purpose: Specifies the possible type of **NT\_SID** (section 2.2.18).

Description: Can be one of the following values:

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

These values are semantically the same as those found in the enumeration **SID\_NAME\_USE**, as defined in [MS-SAMR] section 2.2.2.6.

### 2.2.18 guid Type

Name: **guid**

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

Purpose: Globally unique identifier.

Description: Used to identify various things. Semantically the same as [MS-DTYP] section 2.3.2.1.

### 2.2.19 bool Type

Name : **bool**

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

Type : **boolean** [W3C-XSD2]

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 *Client/Server Details*

No additional detailed interaction between client and server beyond that specified in [RFC2518] applies.

It is important to note that the **descriptor property** (section 2.2.1) does define access control access to the targeted entity. It is possible for the client to set this property in such a way as to deny or grant access to the targeted entity, so care has to be taken to ensure that the access set is what is desired.

Also, it bears reiterating that the **descriptor** property that is retrieved from the server can be more complete than what is required of the client to set it. In section 2.2.1 it is mentioned that the client does not need to set the entire security descriptor in order to just modify the **DACL** (section 2.2.7). Another way that the property might differ is in the **SID** (section 2.2.16) values. The server tries to generate all versions of the identifiers of the security principal, but the client can only generate one of them. It is recommended that the client generate the most precise one as specified in section 2.2.16 in order to be as accurate as possible.

#### 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 client sends a **WebDAV** command that retrieves or sets the value of this **property**. 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** MAY 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_map_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:sid>
        </S:access_allowed_ace>
    </S:effective_aces>
    <S:dacl>
        <S:security_descriptor>
            <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>

```

To set a security descriptor by using the **WebDAV PROPPATCH**, the property 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:effective_aces>
        </S:dacl>
    </S:security_descriptor>
</d:descriptor>

```

```

        </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: Office/Exchange Behavior

The information in this specification is applicable to the following versions of Office/Exchange:

- Microsoft Office 2003
- Microsoft Exchange Server 2003
- Microsoft Office 2007
- Microsoft Exchange Server 2007

Exceptions, if any, are noted below. Unless otherwise specified, any statement of optional behavior in this specification prescribed using the terms SHOULD or SHOULD NOT implies Office/Exchange behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies Office/Exchange does not follow the prescription.

## Index

- Applicability statement, 7
- Client/server details, 24
- Fields, vendor-extensible, 7
- Glossary, 5
- Index of security parameters, 27
- Informative references, 6
- Introduction, 5
- Message syntax, 7
- Messages, 7
- Normative references, 6
- Office/Exchange behavior, 28
- Overview, 6
- Preconditions, 7
- Prerequisites, 7
- Protocol details, 24
  - Client/server details, 24
- Protocol Examples, 25
- References, 6
  - Informative references, 6
  - Normative references, 6
- Relationship to other protocols, 7
- Retrieving the property, 25
- Security, 27
  - Considerations for implementers, 27
  - Index of security parameters, 27
- Security considerations for implementers, 27
- Standards assignments, 7
- Transport, 7
  - Message syntax, 7
- Vendor-extensible fields, 7
- Versioning and capability negotiation, 7