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

**Intellectual Property Rights Notice for Protocol Documentation**

**Tools**. This protocol documentation is intended for use in conjunction with publicly available standard specifications and networking programming art, and assumes that the reader is either 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 a Licensee to develop an implementation. Licensees who have access to Microsoft programming tools and environments 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. |

# Table of Contents

# 1 Introduction

This document specifies an extension to the WebDAV protocol as defined in [RFC2518] by using a standard HTTP mechanism defined in [RFC2068]. This extension specifies how to request and set the Exchange Security Descriptor via WebDAV methods PROPFIND and PROPPATCH.

## 1.1 Glossary

The following terms are defined in [MS-OXGLOS]:

**access control entry (ACE)**
**access control list (ACL)**
**security identifier (SID)**

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 the object.

**entity**: A resource that can be identified by a URL. Use of this term is consistent with that specified in section 2.3 of [RFC2616].

**NT 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 section 2.4.6 of [MS-DTYP].

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

**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", April 2008.

[MS-OXGLOS] Microsoft Corporation, "Office Exchange 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., Frystyk, H., and T. Berners-Lee, "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, 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 (Synopsis)

In WebDAV [RFC2518] properties are able to 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 here.

## 1.4 Relationship to Other Protocols

The descriptor (http://schemas.microsoft.com/exchange/security/descriptor) is a property based on WebDAV 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 it MUST be operated against an entity in 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 section 13 of [RFC2518].

## 2.1 Transport

Messages are transported 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 the W3C [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">
```

```xml
<!-- 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:element name="subcontainer_inheritable_aces"
type="S:inheritable_aces" />
```

```xml
      <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   descriptor Property

Name:        **descriptor**

Namespace:      http://schemas.microsoft.com/exchange/security/
Type:           **security_descriptor** (section 2.2.2)
Purpose:        Contains the **security_descriptor** for entities on the server.
Description:    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, if you want to set only the DACL on an object, set this property 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 as 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 that the server security descriptor is based on. It was designed to be analogous to the SECURITY_DESCRIPTOR [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 defined 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 found 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 semantic that is found 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 found 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 semantic that is found 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 found 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 semantic that is found 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 semantic that is found 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 semantic that is found in [MS-DTYP] section 2.4.6 relating to the Control bit flag DI.

### 2.2.8 sacl Element

Name:    **sacl**
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 found 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 defined in [W3C-XSD2] section 3.3.22

Purpose: This attribute MAY be present for the sacl 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 semantic that is 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 semantic that is 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 semantic that is 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 defined 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 of.

### 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 noncontainer 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 only allowed 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 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 [MS-DTYP] section 2.4.4.

### 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 than 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.

### 2.2.14 access_mask Element

Name: **access_mask**

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

Type: **hexBinary** [W3C-XSD2] section 3.2.15, but limited to between 1 and 8 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. Exchange uses 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 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.

Description: It is important to understand more about the XML representation of NT security identities (SIDs). 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 of the following elements will appear in the representation of the **NT_ Sid** (so long as they are available):

&lt;string_sid&gt;                    (see section 2.2.18.1)
&lt;nt4_compatible_name&gt;    (see section 2.2.18.2)
&lt;type&gt;                          (see section 2.2.18.3)
&lt;ad_object_guid&gt;          (see section 2.2.18.4)
&lt;display_name&gt;              (see section 2.2.18.5)

In some cases less information will be returned.  For instance, 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:

&lt;string_sid&gt;                    (see section 2.2.18.1)
&lt;nt4_compatible_name&gt;    (see section 2.2.18.2)
&lt;ad_object_guid&gt;          (see section 2.2.18.4)
&lt;display_name&gt;              (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 above list – so use **string_sid** if it is known, else nt4_compatible_name, etc.  As a last resort the client MAY use **display_name**, but because of the ambiguity problems it 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 [MS-DTYP] section 2.4.2.

### 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 are found 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).  This element's value is a string representation of the **objectGuid** property found 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).  This element's value is a display name that clients can display in UI. It comes from the PidTagDisplayName as found 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 using this element is that it MAY not be 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 SID. |
| group | A group SID. |
| domain | A domain SID. |
| alias | An alias SID. |
| well_known_group | A SID for a well-known group. |
| deleted_account | A SID for a deleted account. |
| invalid | A SID that is not valid. |

| unknown | A SID of unknown type. |
| computer | A SID for a computer. |

These values are semantically the same as 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 just the values of '0' and '1'.

# 3   Protocol Details

## 3.1   Client/Server Details

No additional detailed interaction between client and server is beyond that as specified in the WebDAV [RFC2518] protocol.

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 MAY 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 attempts to generate all versions of the security principals identifiers, but the client MAY only generate one of them.  It is encouraged that the client generate the most precise one as discussed in the SID 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 as specified in WebDAV [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 WebDAV, 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 WebDAV [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 MAY 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 like:

```
   <d:descriptor  xmlns:d="http://schemas.microsoft.com/exchange/security/">
      <S:security_descriptor
xmlns:S="http://schemas.microsoft.com/security/"
xmlns:D="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/"
D:dt="microsoft.security_descriptor" S:from_mapi_tlh="1">
            <S:revision>1</S:revision>
            <S:owner S:defaulted="0">
              <S:sid>
                <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-
1111</S:string_sid>
                <S:type>user</S:type>
                <S:nt4_compatible_name>ELZCHU-
DOM\bob</S:nt4_compatible_name>
                <S:ad_object_guid>{138bfc4d-48e0-4d29-9de6-
643ecb7314f1}</S:ad_object_guid>
```

```
                  <S:display_name>bob</S:display_name>
                </S:sid>
              </S:owner>
              <S:primary_group S:defaulted="0">
                <S:sid>
                  <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-
513</S:string_sid>
                  <S:type>group</S:type>
                  <S:nt4_compatible_name>ELZCHU-DOM\Domain
Users</S:nt4_compatible_name>
                  <S:ad_object_guid>{f2a02601-c596-4fd2-9543-
d770ba31d9e5}</S:ad_object_guid>
                </S:sid>
              </S:primary_group>
              <S:dacl S:defaulted="1" S:protected="0" S:autoinherited="1">
                <S:revision>2</S:revision>
                <S:effective_aces>
                  <S:access_allowed_ace S:inherited="1">
                    <S:access_mask>1f0fbf</S:access_mask>
                    <S:sid>
                      <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-
500</S:string_sid>
                      <S:type>user</S:type>
                      <S:nt4_compatible_name>ELZCHU-
DOM\Administrator</S:nt4_compatible_name>
                      <S:ad_object_guid>{41a1a32a-4d0f-41ab-ad0c-
fb344ef368fd}</S:ad_object_guid>
                      <S:display_name>Administrator</S:display_name>
                    </S:sid>
                  </S:access_allowed_ace>
                  <S:access_allowed_ace S:inherited="1">
                    <S:access_mask>1f0fbf</S:access_mask>
                    <S:sid>
                      <S:string_sid>S-1-5-7</S:string_sid>
                      <S:type>well_known_group</S:type>
                      <S:nt4_compatible_name>NT AUTHORITY\ANONYMOUS
LOGON</S:nt4_compatible_name>
                      <S:ad_object_guid>{ff158509-ee41-4c44-98c1-
affd7edf6a83}</S:ad_object_guid>
                    </S:sid>
                  </S:access_allowed_ace>
                  <S:access_allowed_ace S:inherited="1">
                    <S:access_mask>1f0fbf</S:access_mask>
                    <S:sid>
                      <S:string_sid>S-1-1-0</S:string_sid>
                      <S:type>well_known_group</S:type>
<S:nt4_compatible_name>\Everyone</S:nt4_compatible_name>
                      <S:ad_object_guid>{aa5d6b3e-3546-4f9e-8530-
59ad567c6dd8}</S:ad_object_guid>
                    </S:sid>
                  </S:access_allowed_ace>
                </S:effective_aces>
              </S:dacl>
            </S:security_descriptor>
```

```
      </d:descriptor>
```

To set a security descriptor using the WebDAV PROPPATCH, the property MAY look like this:

```xml
<?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 any as specified in WebDAV [RFC2518] section 17, HTTP [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 and Exchange:

- Office 2003 with Service Pack 3 applied
- Exchange 2003 with Service Pack 2 applied
- Office 2007 with Service Pack 1 applied
- Exchange 2007 with Service Pack 1 applied

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 Windows behavior in accordance with the SHOULD or SHOULD NOT prescription.  Unless otherwise specified, the term MAY implies that Exchange does not follow the prescription.

# 7   Index