ACE Strings

The security descriptor definition language (SDDL) uses ACE strings in the DACL and SACL components of a *security descriptor* string.

As shown in the Security Descriptor String Format examples, each ACE in a security descriptor string is enclosed in parentheses. The fields of the ACE are in the following order and are separated by semicolons (;).

Note There is a different format for conditional *access control entries* (ACEs) than other ACE types. For conditional ACEs, see Security Descriptor Definition Language for Conditional ACEs.

```
ace_type;ace_flags;rights;object_guid;inherit_object_guid;account_sid;(resource_attribute)
```

Fields

ace_type

A string that indicates the value of the **AceType** member of the **ACE_HEADER** structure. The ACE type string can be one of the following strings defined in Sddl.h.

ACE type string	Constant in Sddl.h	AceType value
"A"	SDDL_ACCESS_ALLOWED	ACCESS_ALLOWED_ACE_TYPE
"D"	SDDL_ACCESS_DENIED	ACCESS_DENIED_ACE_TYPE
"OA"	SDDL_OBJECT_ACCESS_ALLOWED	ACCESS_ALLOWED_OBJECT_ACE_TYPE
"OD"	SDDL_OBJECT_ACCESS_DENIED	ACCESS_DENIED_OBJECT_ACE_TYPE
"AU"	SDDL_AUDIT	SYSTEM_AUDIT_ACE_TYPE
"AL"	SDDL_ALARM	SYSTEM_ALARM_ACE_TYPE
"OU"	SDDL_OBJECT_AUDIT	SYSTEM_AUDIT_OBJECT_ACE_TYPE
"OL"	SDDL_OBJECT_ALARM	SYSTEM_ALARM_OBJECT_ACE_TYPE
"ML"	SDDL_MANDATORY_LABEL	SYSTEM_MANDATORY_LABEL_ACE_TYPE
"XA"	SDDL_CALLBACK_ACCESS_ALLOWED	ACCESS_ALLOWED_CALLBACK_ACE_TYPE **Windows Vista and Windows Server 2003:** Not available.
"XD"	SDDL_CALLBACK_ACCESS_DENIED	ACCESS_DENIED_CALLBACK_ACE_TYPE **Windows Vista and Windows Server 2003:** Not available.
"RA"	SDDL_RESOURCE_ATTRIBUTE	SYSTEM_RESOURCE_ATTRIBUTE_ACE_TYPE **Windows Server 2008 R2, Windows 7, Windows Server 2008, Windows Vista, and Windows Server 2003:** Not available.
"SP"	SDDL_SCOPED_POLICY_ID	SYSTEM_SCOPED_POLICY_ID_ACE_TYPE **Windows Server 2008 R2, Windows 7, Windows Server 2008, Windows Vista, and Windows Server 2003:** Not available.
"XU"	SDDL_CALLBACK_AUDIT	SYSTEM_AUDIT_CALLBACK_ACE_TYPE **Windows Server 2008 R2, Windows 7, Windows Server 2008, Windows Vista, and Windows Server 2003:** Not available.
"ZA"	SDDL_CALLBACK_OBJECT_ACCESS_ALLOWED	ACCESS_ALLOWED_CALLBACK_ACE_TYPE **Windows Server 2008 R2, Windows 7, Windows Server 2008, Windows Vista, and Windows Server 2003:** Not available.

Note If **ace_type** is ACCESS_ALLOWED_OBJECT_ACE_TYPE and neither **object_guid** nor **inherit_object_guid** has a **GUID** specified, then **ConvertStringSecurityDescriptorToSecurityDescriptor** converts **ace_type** to ACCESS_ALLOWED_ACE_TYPE.

ace_flags

A string that indicates the value of the **AceFlags** member of the **ACE_HEADER** structure. The ACE flags string can be a concatenation of the following strings defined in Sddl.h.

ACE flags string	Constant in Sddl.h	AceFlag value
"CI"	SDDL_CONTAINER_INHERIT	CONTAINER_INHERIT_ACE
"OI"	SDDL_OBJECT_INHERIT	OBJECT_INHERIT_ACE
"NP"	SDDL_NO_PROPAGATE	NO_PROPAGATE_INHERIT_ACE
"IO"	SDDL_INHERIT_ONLY	INHERIT_ONLY_ACE

"ID"	SDDL_INHERITED	INHERITED_ACE
"SA"	SDDL_AUDIT_SUCCESS	SUCCESSFUL_ACCESS_ACE_FLAG
"FA"	SDDL_AUDIT_FAILURE	FAILED_ACCESS_ACE_FLAG

rights

A string that indicates the access rights controlled by the ACE. This string can be a hexadecimal string representation of the access rights, such as "0x7800003F", or it can be a concatenation of the following strings.

Access rights string	Constant in Sddl.h	Access right value
Generic access rights		
"GA"	SDDL_GENERIC_ALL	GENERIC_ALL
"GR"	SDDL_GENERIC_READ	GENERIC_READ
"GW"	SDDL_GENERIC_WRITE	GENERIC_WRITE
"GX"	SDDL_GENERIC_EXECUTE	GENERIC_EXECUTE
Standard access rights		
"RC"	SDDL_READ_CONTROL	READ_CONTROL
"SD"	SDDL_STANDARD_DELETE	DELETE
"WD"	SDDL_WRITE_DAC	WRITE_DAC
"WO"	SDDL_WRITE_OWNER	WRITE_OWNER
Directory service object access rights		
"RP"	SDDL_READ_PROPERTY	ADS_RIGHT_DS_READ_PROP
"WP"	SDDL_WRITE_PROPERTY	ADS_RIGHT_DS_WRITE_PROP
"CC"	SDDL_CREATE_CHILD	ADS_RIGHT_DS_CREATE_CHILD
"DC"	SDDL_DELETE_CHILD	ADS_RIGHT_DS_DELETE_CHILD
"LC"	SDDL_LIST_CHILDREN	ADS_RIGHT_ACTRL_DS_LIST
"SW"	SDDL_SELF_WRITE	ADS_RIGHT_DS_SELF
"LO"	SDDL_LIST_OBJECT	ADS_RIGHT_DS_LIST_OBJECT
"DT"	SDDL_DELETE_TREE	ADS_RIGHT_DS_DELETE_TREE
"CR"	SDDL_CONTROL_ACCESS	ADS_RIGHT_DS_CONTROL_ACCESS
File access rights		
"FA"	SDDL_FILE_ALL	FILE_ALL_ACCESS
"FR"	SDDL_FILE_READ	FILE_GENERIC_READ
"FW"	SDDL_FILE_WRITE	FILE_GENERIC_WRITE
"FX"	SDDL_FILE_EXECUTE	FILE_GENERIC_EXECUTE
Registry key access rights		
"KA"	SDDL_KEY_ALL	KEY_ALL_ACCESS
"KR"	SDDL_KEY_READ	KEY_READ
"KW"	SDDL_KEY_WRITE	KEY_WRITE
"KX"	SDDL_KEY_EXECUTE	KEY_EXECUTE
Mandatory label rights		
"NR"	SDDL_NO_READ_UP	SYSTEM_MANDATORY_LABEL_NO_READ_UP
"NW"	SDDL_NO_WRITE_UP	SYSTEM_MANDATORY_LABEL_NO_WRITE_UP
"NX"	SDDL_NO_EXECUTE_UP	SYSTEM_MANDATORY_LABEL_NO_EXECUTE_UP

object_guid

A string representation of a GUID that indicates the value of the **ObjectType** member of an object-specific ACE structure, such as **ACCESS_ALLOWED_OBJECT_ACE**. The GUID string

uses the format returned by the **UuidToString** function.

The following table lists some commonly used object GUIDs.

Rights and GUID	Permission
CR;ab721a53-1e2f-11d0-9819-00aa0040529b	Change password
CR;00299570-246d-11d0-a768-00aa006e0529	Reset password

inherit_object_guid
A string representation of a GUID that indicates the value of the **InheritedObjectType** member of an object-specific ACE structure. The GUID string uses the **UuidToString** format.

account_sid
SID string that identifies the trustee of the ACE.

resource_attribute
[OPTIONAL] The resource_attribute is only for resource ACEs and is optional. A string that indicates the data type. The resource attribute ace data type can be one of the following data types defined in Sddl.h.

The "#" sign is synonymous with "0" in resource attributes. For example, D:AI(XA;OICI;FA;;;WD;(OctetStringType==#1#2#3##)) is equivalent to and interpreted as D:AI(XA;OICI;FA;;;WD;(OctetStringType==#01020300)).

Windows Server 2008 R2, Windows 7, Windows Server 2008, Windows Vista, and Windows Server 2003: Resource attributes are not available.

Resource attribute ace data type string	Constant in Sddl.h	Data type
"TI"	SDDL_INT	Signed integer
"TU"	SDDL_UINT	Unsigned integer
"TS"	SDDL_WSTRING	Wide string
"TD"	SDDL_SID	SID
"TX"	SDDL_BLOB	Octet string
"TB"	SDDL_BOOLEAN	Boolean

The following example shows an ACE string for an access-allowed ACE. It is not an object-specific ACE, so it has no information in the **object_guid** and **inherit_object_guid** fields. The **ace_flags** field is also empty, which indicates that none of the ACE flags are set.

C++

```
(A;;RPWPCCDCLCSWRCWDWOGA;;;S-1-0-0)
```

The ACE string shown above describes the following ACE information.

C++

```
AceType:       0x00 (ACCESS_ALLOWED_ACE_TYPE)
AceFlags:      0x00
Access Mask:   0x100e003f
                    READ_CONTROL
                    WRITE_DAC
                    WRITE_OWNER
                    GENERIC_ALL
                    Other access rights(0x0000003f)
Ace Sid      : (S-1-0-0)
```

The following example shows a file classified with resource claims for Windows and Structured Query Language (SQL) with Secrecy set to High Business Impact.

C++

```
(RA;CI;;;;S-1-0-0; ("Project",TS,0,"Windows","SQL"))
(RA;CI;;;;S-1-0-0; ("Secrecy",TU,0,3))
```

The ACE string shown above describes the following ACE information.

C++

```
AceType:       0x12 (SYSTEM_RESOURCE_ATTRIBUTE_ACE_TYPE)
AceFlags:      0x1  (SDDL_CONTAINER_INHERIT)
Access Mask:   0x0
```

```
Ace Sid      : (S-1-0-0)
Resource Attributes: Project has the strings Windows and SQL, Secrecy has the unsigned int value of 3
```

For more information, see Security Descriptor String Format and SID Strings. For conditional ACEs, see Security Descriptor Definition Language for Conditional ACEs.

Related topics

[MS-DTYP]: Security Descriptor Description Language

Community Additions