



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking “Manage Cookies” at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies

Microsoft Ignite

Nov 19–22, 2024

Register now >



Learn

Discover ▾

Product documentation ▾

Development languages ▾

Topics ▾



Sign in

Windows App Development

Explore ▾

Development ▾

Platforms ▾

Troubleshooting

Resources ▾

Dashboard

Filter by title

Authorization

▾ About Authorization

About Authorization

▾ Access Control

Access Control

C2-level Security

> Access Control Model

▾ Security Descriptor Definition Language

Security Descriptor Definition

Language

Security Descriptor String Format

Security Descriptor Definition

Language for Conditional ACEs.

ACE Strings

SID Strings

Privileges

Audit Generation

Securable Objects

> Low-level Access Control

> Access Control Editor

> Client/Server Access Control

> Access Control for Application Resources

> AppContainer

Mandatory Integrity Control

> User Account Control

> Using Authorization in C++

> Using Authorization in Script

> Using Authz API

> Authorization Reference

> Microsoft.Interop.Security.AzRoles Assembly

... / Security and Identity / Authorization /



SID Strings

Article • 09/26/2023 • 7 contributors

Feedback

In the [security descriptor definition language](#) (SDDL), [security descriptor string](#) use SID strings for the following components of a [security descriptor](#):

- Owner
- Primary group
- The [trustee](#) in an ACE

A SID string in a security descriptor string can use either the standard string representation of a SID (*S-R-I-S-S*) or one of the string constants defined in Sddl.h. For more information about the standard SID string notation, see [SID Components](#).

The following SID string constants for well-known SIDs are defined in Sddl.h. For information about the corresponding [relative IDs](#) (RIDs), see [Well-known SIDs](#).

Expand table

SDDL SID string	Constant in Sddl.h	Account alias and corresponding RID
"AA"	SDDL_ACCESS_CONTROL_ASSISTANCE_OPS	Access control assistance operators. The corresponding RID is DOMAIN_ALIAS_RID_ACCESS_CONTROL_ASSISTANCE_OPS. Server 2008 R2, Windows 7, Windows Server 2012 R2, Windows Server 2016: Not available.
"AC"	SDDL_ALL_APP_PACKAGES	All applications running in an app package context. The corresponding RID is SECURITY_BUILTIN_PACKAGE_ANY_PACKAGE. Server 2008 R2, Windows 7, Windows Server 2008, Windows Server 2012 R2, Windows Server 2016: Not available.
"AN"	SDDL_ANONYMOUS	Anonymous logon. The corresponding RID is SECURITY_ANONYMOUS_LOGON_RID.
"AO"	SDDL_ACCOUNT_OPERATORS	Account operators. The corresponding RID is DOMAIN_ALIAS_RID_ACCOUNT_OPS.
"AP"	SDDL_PROTECTED_USERS	Protected Users . The corresponding RID is DOMAIN_GROUP_RID_PROTECTED_USERS. Windows 8, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 10, Windows 11, Windows Server 2022: Not available.

 Download PDF

"AU"	SDDL_AUTHENTICATED_USERS	Authenticated users. The corresponding RID is SECURITY_AUTHENTICATED_USER_RID.
"BA"	SDDL_BUILTIN_ADMINISTRATORS	Built-in administrators. The corresponding RID is DOMAIN_ALIAS_RID_ADMINS.
"BG"	SDDL_BUILTIN_GUESTS	Built-in guests. The corresponding RID is DOMAIN_ALIAS_RID_GUESTS.
"BO"	SDDL_BACKUP_OPERATORS	Backup operators. The corresponding RID is DOMAIN_ALIAS_RID_BACKUP_OPS.
"BU"	SDDL_BUILTIN_USERS	Built-in users. The corresponding RID is DOMAIN_ALIAS_RID_USERS.
"CA"	SDDL_CERT_SERV_ADMINISTRATORS	Certificate publishers. The corresponding RID is DOMAIN_GROUP_RID_CERT_ADMINS.
"CD"	SDDL_CERTSVC_DCOM_ACCESS	Users who can connect to certification authorities Component Object Model (DCOM). The corresponding RID is DOMAIN_ALIAS_RID_CERTSVC_DCOM_ACCESS. Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows 8, Windows 8.1, Windows Server 2012, Windows 10, Windows 11: Not available.
"CG"	SDDL_CREATOR_GROUP	Creator group. The corresponding RID is SECURITY_CREATOR_GROUP_RID.
"CN"	SDDL_CLONEABLE_CONTROLLERS	Cloneable domain controllers. The corresponding RID is DOMAIN_GROUP_RID_CLONEABLE_CONTROLLERS. Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows 8, Windows 8.1, Windows Server 2012, Windows 10, Windows 11: Not available.
"CO"	SDDL_CREATOR_OWNER	Creator owner. The corresponding RID is SECURITY_CREATOR_OWNER_RID.
"CY"	SDDL_CRYPTO_OPERATORS	Crypto operators. The corresponding RID is DOMAIN_ALIAS_RID_CRYPTO_OPERATORS. Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows 8, Windows 8.1, Windows Server 2012, Windows 10, Windows 11: Not available.
"DA"	SDDL_DOMAIN_ADMINISTRATORS	Domain administrators. The corresponding RID is DOMAIN_GROUP_RID_ADMINS.
"DC"	SDDL_DOMAIN_COMPUTERS	Domain computers. The corresponding RID is DOMAIN_GROUP_RID_COMPUTERS.
"DD"	SDDL_DOMAIN_DOMAIN_CONTROLLERS	Domain controllers. The corresponding RID is DOMAIN_GROUP_RID_CONTROLLERS.
"DG"	SDDL_DOMAIN_GUESTS	Domain guests. The corresponding RID is DOMAIN_ALIAS_RID_GUESTS.
"DU"	SDDL_DOMAIN_USERS	Domain users. The corresponding RID is DOMAIN_ALIAS_RID_USERS.
"EA"	SDDL_ENTERPRISE_ADMINS	Enterprise administrators. The corresponding RID is DOMAIN_GROUP_RID_ENTERPRISE_ADMINS.
"ED"	SDDL_ENTERPRISE_DOMAIN_CONTROLLERS	Enterprise domain controllers. The corresponding RID is SECURITY_SERVER_LOGON_RID.
"EK"	SDDL_ENTERPRISE_KEY_ADMINS	Enterprise key admins. The corresponding RID is DOMAIN_GROUP_RID_ENTERPRISE_KEY_ADMINS. Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows 8, Windows 8.1, Windows Server 2012, Windows 10, Windows 11: Not available.
"ER"	SDDL_EVENT_LOG_READERS	Event log readers. The corresponding RID is DOMAIN_ALIAS_RID_EVENT_LOG_READERS_GRP. Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows 8, Windows 8.1, Windows Server 2012, Windows 10, Windows 11: Not available.
"ES"	SDDL_RDS_ENDPOINT_SERVERS	Endpoint servers. The corresponding RID is DOMAIN_ALIAS_RID_RDS_ENDPOINT_SERVERS. Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows 8, Windows 8.1, Windows Server 2012, Windows 10, Windows 11: Not available.
"HA"	SDDL_HYPER_V_ADMINS	Hyper-V administrators. The corresponding RID is DOMAIN_ALIAS_RID_HYPER_V_ADMINS. Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows 8, Windows 8.1, Windows Server 2012, Windows 10, Windows 11: Not available.

"HI"	SDDL_ML_HIGH	High integrity level. The corresponding RID is SECURITY_MANDATORY_HIGH_RID. Windows Se
"HO"	SDDL_USER_MODE_HARDWARE_OPERATORS	Group members may operate hardware from use corresponding RID is DOMAIN_ALIAS_RID_USER_MODE_HARDWARE_O
"IS"	SDDL_IIS_USERS	Anonymous Internet users. The corresponding RI DOMAIN_ALIAS_RID_IUSERS. Windows Server 2
"IU"	SDDL_INTERACTIVE	Interactively logged-on user. This is a group iden of a process when it was logged on interactively. type is LOGON32_LOGON_INTERACTIVE. The co SECURITY_INTERACTIVE_RID.
"KA"	SDDL_KEY_ADMINS	Domain key admins. The corresponding RID is DOMAIN_GROUP_RID_KEY_ADMINS. Windows 9 Windows 8.1, Windows Server 2012, Windows 8 R2, Windows 7, Windows Server 2008, Window Server 2003: Not available.
"LA"	SDDL_LOCAL_ADMIN	Local administrator. The corresponding RID is DOMAIN_USER_RID_ADMIN.
"LG"	SDDL_LOCAL_GUEST	Local guest. The corresponding RID is DOMAIN_U
"LS"	SDDL_LOCAL_SERVICE	Local service account. The corresponding RID is SECURITY_LOCAL_SERVICE_RID.
"LU"	SDDL_PERFLOG_USERS	Performance Log users. The corresponding RID is DOMAIN_ALIAS_RID_LOGGING_USERS.
"LW"	SDDL_ML_LOW	Low integrity level. The corresponding RID is SECURITY_MANDATORY_LOW_RID. Windows Se
"ME"	SDDL_ML_MEDIUM	Medium integrity level. The corresponding RID is SECURITY_MANDATORY_MEDIUM_RID. Window available.
"MP"	SDDL_ML_MEDIUM_PLUS	Medium Plus integrity level. The corresponding R SECURITY_MANDATORY_MEDIUM_PLUS_RID. W Windows Vista and Windows Server 2003: Not .
"MU"	SDDL_PERFMON_USERS	Performance Monitor users. The corresponding R DOMAIN_ALIAS_RID_MONITORING_USERS.
"NO"	SDDL_NETWORK_CONFIGURATION_OPS	Network configuration operators. The corresponc DOMAIN_ALIAS_RID_NETWORK_CONFIGURATIC
"NS"	SDDL_NETWORK_SERVICE	Network service account. The corresponding RID SECURITY_NETWORK_SERVICE_RID.
"NU"	SDDL_NETWORK	Network logon user. This is a group identifier add process when it was logged on across a network. type is LOGON32_LOGON_NETWORK. The corre SECURITY_NETWORK_RID.
"OW"	SDDL_OWNER_RIGHTS	Owner Rights SID. The corresponding RID is SECURITY_CREATOR_OWNER_RIGHTS_RID. <i>Wind</i> available.
"PA"	SDDL_GROUP_POLICY_ADMINS	Group Policy administrators. The corresponding F DOMAIN_GROUP_RID_POLICY_ADMINS.
"PO"	SDDL_PRINTER_OPERATORS	Printer operators. The corresponding RID is DOMAIN_ALIAS_RID_PRINT_OPS
"PS"	SDDL_PERSONAL_SELF	Principal self. The corresponding RID is SECURITY
"PU"	SDDL_POWER_USERS	Power users. The corresponding RID is DOMAIN_ALIAS_RID_POWER_USERS.
"RA"	SDDL_RDS_REMOTE_ACCESS_SERVERS	RDS remote access servers. The corresponding RI DOMAIN_ALIAS_RID_RDS_REMOTE_ACCESS_SER

		2008 R2, Windows 7, Windows Server 2008, Windows Server 2003: Not available.
"RC"	SDDL_RESTRICTED_CODE	Restricted code. This is a restricted token created CreateRestrictedToken function. The corresponding RID is SECURITY_RESTRICTED_CODE_RID.
"RD"	SDDL_REMOTE_DESKTOP	Terminal server users. The corresponding RID is DOMAIN_ALIAS_RID_REMOTE_DESKTOP_USERS.
"RE"	SDDL_REPLICATOR	Replicator. The corresponding RID is DOMAIN_ALIAS_RID_REPLICATOR.
"RM"	SDDL_RMS__SERVICE_OPERATORS	RMS Service. Available only in Windows Vista.
"RO"	SDDL_ENTERPRISE_RO_DCs	Enterprise Read-only domain controllers. The corresponding RID is DOMAIN_GROUP_RID_ENTERPRISE_READONLY. Windows Server 2008, Windows Vista and Windows 7: Available.
"RS"	SDDL_RAS_SERVERS	RAS servers group. The corresponding RID is DOMAIN_ALIAS_RID_RAS_SERVERS.
"RU"	SDDL_ALIAS_PREW2KCOMPACC	Alias to grant permissions to accounts that use a with operating systems previous to Windows 2000. The corresponding RID is DOMAIN_ALIAS_RID_PREW2KCOMPACC.
"SA"	SDDL_SCHEMA ADMINISTRATORS	Schema administrators. The corresponding RID is DOMAIN_GROUP_RID_SCHEMA_ADMINS.
"SI"	SDDL_ML_SYSTEM	System integrity level. The corresponding RID is SECURITY_MANDATORY_SYSTEM_RID. Windows Vista and Windows 7: Available.
"SO"	SDDL_SERVER_OPERATORS	Server operators. The corresponding RID is DOMAIN_ALIAS_RID_SYSTEM_OPS.
"SS"	SDDL_SERVICE_ASSERTED	Authentication service asserted. The corresponding RID is SECURITY_AUTHENTICATION_SERVICE_ASSERTED. Windows Server 2008 R2, Windows 7, Windows Server 2008, Windows Server 2003: Not available.
"SU"	SDDL_SERVICE	Service logon user. This is a group identifier added to the process when it was logged as a service. The corresponding RID is LOGON32_LOGON_SERVICE. The corresponding RID is SECURITY_SERVICE_RID.
"SY"	SDDL_LOCAL_SYSTEM	Local system. The corresponding RID is SECURITY_LOCAL_SYSTEM_RID.
"UD"	SDDL_USER_MODE_DRIVERS	User-mode driver. The corresponding RID is SECURITY_USERMODEDRIVERHOST_ID_BASE_RID. Windows Server 2008 R2, Windows 7, Windows Server 2008, Windows Server 2003: Not available.
"WD"	SDDL_EVERYONE	Everyone. The corresponding RID is SECURITY_WORLD_RID.
"WR"	SDDL_WRITE_RESTRICTED_CODE	Write Restricted code. The corresponding RID is SECURITY_WRITE_RESTRICTED_CODE_RID. Windows Vista and Windows 7: Available.

The [ConvertSidToStringSid](#) and [ConvertStringSidToSid](#) functions always use the standard SID string notation and do not support SDDL SID string constants.

For more information about well-known SIDs, see [Well-known SIDs](#).

See also

[\[MS-DTYP\]: Security Descriptor Description Language](#)

Feedback

Was this page helpful?

👍 Yes

👎 No



[Provide product feedback](#) | [Get help at Microsoft Q&A](#)

Additional resources

Events

Nov 20, 12 AM - Nov 22, 12 AM

Gain the competitive edge you need with powerful AI and Cloud solutions by attending Microsoft Ignite online.
[Register now](#)

 English (United States)  Your Privacy Choices  Theme 

[Manage cookies](#) [Previous Versions](#) [Blog](#) [Contribute](#) [Privacy](#) [Terms of Use](#) [Trademarks](#) © Microsoft 2024