Microsoft Windows SID's

For more information contact: info@syntricate.com

Well-known SIDs:

- SID: S-1-0
  Name: Null Authority
  Description: An identifier authority.
- SID: S-1-0-0
  Name: Nobody
  Description: No security principal.
- SID: S-1-1
  Name: World Authority
  Description: An identifier authority.
- SID: S-1-1-0
  Name: Everyone
  Description: A group that includes all users, even anonymous users and guests. Membership is controlled by the operating system.
  Note By default, the Everyone group no longer includes anonymous users on a computer that is running Windows XP Service Pack 2 (SP2).
- SID: S-1-2
  Name: Local Authority
  Description: An identifier authority.
- SID: S-1-2-0
  Name: Local
  Description: A group that includes all users who have logged on locally.
- SID: S-1-2-1
  Name: Console Logon
  Description: A group that includes users who are logged on to the physical console.
  Note Added in Windows 7 and Windows Server 2008 R2

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-3
  Name: Creator Authority
  Description: An identifier authority.
- SID: S-1-3-0
  Name: Creator Owner
  Description: A placeholder in an inheritable access control entry (ACE). When the ACE is inherited, the system replaces this SID with the SID for the object's creator.
- SID: S-1-3-1
  Name: Creator Group
  Description: A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the primary group of the object's creator. The primary group is used only by the POSIX subsystem.
- SID: S-1-3-2
  Name: Creator Owner Server
  Description: This SID is not used in Windows 2000.
- SID: S-1-3-3
  Name: Creator Group Server
  Description: This SID is not used in Windows 2000.
- SID: S-1-3-4 Name: Owner Rights
  Description: A group that represents the current owner of the object. When an ACE that carries this SID is applied to an object, the system ignores the implicit READ_CONTROL and WRITE_DAC permissions for the object owner.
  Note Added in Windows Vista and Windows Server 2008
- SID: S-1-4
  Name: Non-unique Authority
  Description: An identifier authority.

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-5
  Name: NT Authority
  Description: An identifier authority.
- SID: S-1-5-1
  Name: Dialup
  Description: A group that includes all users who have logged on through a dial-up connection. Membership is controlled by the operating system.
- SID: S-1-5-2
  Name: Network
  Description: A group that includes all users that have logged on through a network connection. Membership is controlled by the operating system.
- SID: S-1-5-3
  Name: Batch
  Description: A group that includes all users that have logged on through a batch queue facility. Membership is controlled by the operating system.
- SID: S-1-5-4
  Name: Interactive
  Description: A group that includes all users that have logged on interactively. Membership is controlled by the operating system.
- SID: S-1-5-5-X-Y
  Name: Logon Session
  Description: A logon session. The X and Y values for these SIDs are different for each session.
- SID: S-1-5-6
  Name: Service
  Description: A group that includes all security principals that have logged on as a service. Membership is controlled by the operating system.

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-5-7
  Name: Anonymous
  Description: A group that includes all users that have logged on anonymously. Membership is controlled by the operating system.
- SID: S-1-5-8
  Name: Proxy
  Description: This SID is not used in Windows 2000.
- SID: S-1-5-9
  Name: Enterprise Domain Controllers
  Description: A group that includes all domain controllers in a forest that uses an Active Directory directory service. Membership is controlled by the operating system.
- SID: S-1-5-10
  Name: Principal Self
  Description: A placeholder in an inheritable ACE on an account object or group object in Active Directory. When the ACE is inherited, the system replaces this SID with the SID for the security principal who holds the account.
- SID: S-1-5-11
  Name: Authenticated Users
  Description: A group that includes all users whose identities were authenticated when they logged on. Membership is controlled by the operating system.
- SID: S-1-5-12
  Name: Restricted Code
  Description: This SID is reserved for future use.
- SID: S-1-5-13
  Name: Terminal Server Users
  Description: A group that includes all users that have logged on to a Terminal Services server. Membership is controlled by the operating system.

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-5-14
  Name: Remote Interactive Logon
  Description: A group that includes all users who have logged on through a terminal services logon.
- SID: S-1-5-15
  Name: This Organization
  Description: A group that includes all users from the same organization. Only included with AD accounts and only added by a Windows Server 2003 or later domain controller.
- SID: S-1-5-17
  Name: This Organization
  Description: An account that is used by the default Internet Information Services (IIS) user.
- SID: S-1-5-18
  Name: Local System
  Description: A service account that is used by the operating system.
- SID: S-1-5-19
  Name: NT Authority
  Description: Local Service
- SID: S-1-5-20
  Name: NT Authority
  Description: Network Service
- SID: S-1-5-21*domain*-500
  Name: Administrator
  Description: A user account for the system administrator. By default, it is the only user account that is given full control over the system.
- SID: S-1-5-21*domain*-501
  Name: Guest
  Description: A user account for people who do not have individual accounts. This user account does not require a password. By default, the Guest account is disabled.

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-5-21*domain*-502
  Name: KRBTGT
  Description: A service account that is used by the Key Distribution Center (KDC) service.
- SID: S-1-5-21*domain*-512
  Name: Domain Admins
  Description: A global group whose members are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. Domain Admins is the default owner of any object that is created by any member of the group.
- SID: S-1-5-21*domain*-513
  Name: Domain Users
  Description: A global group that, by default, includes all user accounts in a domain. When you create a user account in a domain, it is added to this group by default.
- SID: S-1-5-21*domain*-514
  Name: Domain Guests
  Description: A global group that, by default, has only one member, the domain's built-in Guest account.
- SID: S-1-5-21*domain*-515
  Name: Domain Computers
  Description: A global group that includes all clients and servers that have joined the domain.
- SID: S-1-5-21*domain*-516
  Name: Domain Controllers
  Description: A global group that includes all domain controllers in the domain. New domain controllers are added to this group by default.

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-5-21*domain*-517
  Name: Cert Publishers
  Description: A global group that includes all computers that are running an enterprise certification authority. Cert Publishers are authorized to publish certificates for User objects in Active Directory.
- SID: S-1-5-21*root domain*-518
  Name: Schema Admins
  Description: A universal group in a native-mode domain; a global group in a mixed-mode domain. The group is authorized to make schema changes in Active Directory. By default, the only member of the group is the Administrator account for the forest root domain.
- SID: S-1-5-21*root domain*-519
  Name: Enterprise Admins
  Description: A universal group in a native-mode domain; a global group in a mixed-mode domain. The group is authorized to make forest-wide changes in Active Directory, such as adding child domains. By default, the only member of the group is the Administrator account for the forest root domain.
- SID: S-1-5-21*domain*-520
  Name: Group Policy Creator Owners
  Description: A global group that is authorized to create new Group Policy objects in Active Directory. By default, the only member of the group is Administrator.
- SID: S-1-5-21*domain*-553
  Name: RAS and IAS Servers
  Description: A domain local group. By default, this group has no members. Servers in this group have Read Account Restrictions and Read Logon Information access to User objects in the Active Directory domain local group.

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-5-32-544
  Name: Administrators
  Description: A built-in group. After the initial installation of the operating system, the only member of the group is the Administrator account. When a computer joins a domain, the Domain Admins group is added to the Administrators group. When a server becomes a domain controller, the Enterprise Admins group also is added to the Administrators group.
- SID: S-1-5-32-545
  Name: Users
  Description: A built-in group. After the initial installation of the operating system, the only member is the Authenticated Users group. When a computer joins a domain, the Domain Users group is added to the Users group on the computer.
- SID: S-1-5-32-546
  Name: Guests
  Description: A built-in group. By default, the only member is the Guest account. The Guests group allows occasional or one-time users to log on with limited privileges to a computer's built-in Guest account.
- SID: S-1-5-32-547
  Name: Power Users
  Description: A built-in group. By default, the group has no members. Power users can create local users and groups; modify and delete accounts that they have created; and remove users from the Power Users, Users, and Guests groups. Power users also can install programs; create, manage, and delete local printers; and create and delete file shares.

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-5-32-548
  Name: Account Operators
  Description: A built-in group that exists only on domain controllers. By default, the group has no members. By default, Account Operators have permission to create, modify, and delete accounts for users, groups, and computers in all containers and organizational units of Active Directory except the Built-in container and the Domain Controllers OU. Account Operators do not have permission to modify the Administrators and Domain Admins groups, nor do they have permission to modify the accounts for members of those groups.
- SID: S-1-5-32-549
  Name: Server Operators
  Description: A built-in group that exists only on domain controllers. By default, the group has no members. Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back-up and restore files; format the hard disk of the computer; and shut down the computer.
- SID: S-1-5-32-550
  Name: Print Operators
  Description: A built-in group that exists only on domain controllers. By default, the only member is the Domain Users group. Print Operators can manage printers and document queues.
- SID: S-1-5-32-551
  Name: Backup Operators
  Description: A built-in group. By default, the group has no members. Backup Operators can back up and restore all files on a computer, regardless of the permissions that protect those files. Backup Operators also can log on to the computer and shut it down.

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-5-32-552
  Name: Replicators
  Description: A built-in group that is used by the File Replication service on domain controllers. By default, the group has no members. Do not add users to this group.
- SID: S-1-5-64-10
  Name: NTLM Authentication
  Description: A SID that is used when the NTLM authentication package authenticated the client
- SID: S-1-5-64-14
  Name: SChannel Authentication
  Description: A SID that is used when the SChannel authentication package authenticated the client.
- SID: S-1-5-64-21
  Name: Digest Authentication
  Description: A SID that is used when the Digest authentication package authenticated the client.
- SID: S-1-5-80
  Name: NT Service
  Description: An NT Service account prefix
- SID: S-1-16-0
  Name: Untrusted Mandatory Level
  Description: An untrusted integrity level. Note Added in Windows Vista and Windows Server 2008
  Note Added in Windows Vista and Windows Server 2008

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-16-4096
  Name: Low Mandatory Level
  Description: A low integrity level.
  Note Added in Windows Vista and Windows Server 2008
- SID: S-1-16-8192
  Name: Medium Mandatory Level
  Description: A medium integrity level.
  Note Added in Windows Vista and Windows Server 2008
- SID: S-1-16-8448
  Name: Medium Plus Mandatory Level
  Description: A medium plus integrity level.
  Note Added in Windows Vista and Windows Server 2008
- SID: S-1-16-12288
  Name: High Mandatory Level
  Description: A high integrity level.
  Note Added in Windows Vista and Windows Server 2008
- SID: S-1-16-16384
  Name: System Mandatory Level
  Description: A system integrity level.
  Note Added in Windows Vista and Windows Server 2008
- SID: S-1-16-20480
  Name: Protected Process Mandatory Level
  Description: A protected-process integrity level.
  Note Added in Windows Vista and Windows Server 2008

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-16-28672
  Name: Secure Process Mandatory Level
  Description: A secure process integrity level.
  Note Added in Windows Vista and Windows Server 2008
- SID: S-1-5-80-0
  SID S-1-5-80-0 = NT SERVICES\ALL SERVICES
  Name: All Services
  Description: A group that includes all service processes that are configured on the system. Membership is controlled by the operating system.
  Note Added in Windows Server 2008 R2
  The following groups will show as SIDs until a Windows Server 2003 domain controller is made the primary domain controller (PDC) operations master role holder. (The "operations master" is also known as flexible single master operations or FSMO.)
  Additional new built-in groups that are created when a Windows Server 2003 domain controller is added to the domain are:
- SID: S-1-5-32-554
  Name: BUILT-IN\Pre-Windows 2000 Compatible Access
  Description: An alias added by Windows 2000. A backward compatibility group which allows read access on all users and groups in the domain.
- SID: S-1-5-32-555
  Name: BUILT-IN\Remote Desktop Users
  Description: An alias. Members in this group are granted the right to logon remotely.
- SID: S-1-5-32-556
  Name: BUILT-IN\Network Configuration Operators
  Description: An alias. Members in this group can have some administrative privileges to manage configuration of networking features.

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-5-32-557
  Name: BUILT-IN\Incoming Forest Trust Builders
  Description: An alias. Members of this group can create incoming, one-way trusts to this forest.
- SID: S-1-5-32-558
  Name: BUILT-IN\Performance Monitor Users
  Description: An alias. Members of this group have remote access to monitor this computer.
- SID: S-1-5-32-559
  Name: BUILT-IN\Performance Log Users
  Description: An alias. Members of this group have remote access to schedule logging of performance counters on this computer.
- SID: S-1-5-32-560
  Name: BUILT-IN\Windows Authorization Access Group
  Description: An alias. Members of this group have access to the computed token Groups Global And Universal attribute on User objects.
- SID: S-1-5-32-561
  Name: BUILT-IN\Terminal Server License Servers
  Description: An alias. A group for Terminal Server License Servers. When Windows Server 2003 Service Pack 1 is installed, a new local group is created.
- SID: S-1-5-32-562
  Name: BUILT-IN\Distributed COM Users
  Description: An alias. A group for COM to provide computer wide access controls that govern access to all call, activation, or launch requests on the computer.

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

The following groups will show as SIDs until a Windows Server 2008 or Windows Server 2008 R2 domain controller is made the primary domain controller (PDC) operations master role holder. (The "operations master" is also known as flexible single master operations or FSMO.) Additional new built-in groups that are created when a Windows Server 2008 or Windows Server 2008 R2 domain controller is added to the domain are:

- SID: S-1-5- 21*domain* -498
  Name: Enterprise Read-only Domain Controllers
  Description: A Universal group. Members of this group are Read-Only Domain Controllers in the enterprise
- SID: S-1-5- 21*domain* -521
  Name: Read-only Domain Controllers
  Description: A Global group. Members of this group are Read-Only Domain Controllers in the domain
- SID: S-1-5-32-569
  Name: BUILT-IN\Cryptographic Operators
  Description: A Built-in Local group. Members are authorized to perform cryptographic operations.
- SID: S-1-5-21 *domain* -571
  Name: Allowed RODC Password Replication Group
  Description: A Domain Local group. Members in this group can have their passwords replicated to all read-only domain controllers in the domain.
- SID: S-1-5- 21 *domain* -572
  Name: Denied RODC Password Replication Group
  Description: A Domain Local group. Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain

SYNTRICATE

Microsoft Windows SID's

For more information contact: info@syntricate.com

- SID: S-1-5-32-573
  Name: BUILT-IN\Event Log Readers
  Description: A Built-in Local group. Members of this group can read event logs from local machine.
- SID: S-1-5-32-574
  Name: BUILT-IN\Certificate Service DCOM Access
  Description: A Built-in Local group. Members of this group are allowed to connect to Certification Authorities in the enterprise.

SYNTRICATE