Security Identifiers

By robinharwood

Archived: 2026-04-05 16:46:19 UTC

This article describes how security identifiers (SIDs) work with accounts and groups in the Windows Server operating system.

What are SIDs?

A SID is used to uniquely identify a security principal or security group. Security principals can represent any entity that the operating system can authenticate. Examples include a user account, a computer account, or a thread or process that runs in the security context of a user or computer account.

Each account or group, or each process that runs in the security context of the account, has a unique SID that's issued by an authority, such as a Windows domain controller. The SID is stored in a security database. The system generates the SID that identifies a particular account or group at the time the account or group is created. When a SID is used as the unique identifier for a user or group, it can never be used again to identify another user or group.

Each time a user signs in, the system creates an access token for that user. The access token contains the user's SID, user rights, and the SIDs for any groups the user belongs to. This token provides the security context for whatever actions the user performs on that computer.

In addition to the uniquely created domain-specific SIDs that are assigned to specific users and groups, there are well-known SIDs that identify generic groups and generic users. For example, the Everyone and World SIDs each identify a group that includes all users. Well-known SIDs have values that remain constant across all operating systems.

SIDs are a fundamental building block of the Windows security model. They work with specific components of the authorization and access control technologies in the security infrastructure of the Windows Server operating systems. This design helps protect access to network resources and provides a more secure computing environment.

Note

This content pertains only to the Windows versions in the "Applies to" list at the beginning of the article.

How SIDs work

Users refer to accounts by the account name. Internally, the operating system refers to accounts and processes that run in the security context of the account by using their SIDs. For domain accounts, the SID of a security principal is created by concatenating the SID of the domain with a relative identifier (RID) for the account. SIDs are unique within their scope (domain or local), and they're never reused.

The operating system generates a SID that identifies a particular account or group at the time the account or group is created. For a local account or group, the Local Security Authority (LSA) on the computer generates the SID. The SID is stored with other account information in a secure area of the registry. For a domain account or group, the domain security authority generates the SID. This type of SID is stored as an attribute of the User or Group object in Active Directory Domain Services.

For every local account and group, the SID is unique for the computer where it's created. No two accounts or groups on the computer ever share the same SID. Likewise, for every domain account and group, the SID is unique within an enterprise. As a result, the SID of an account or group in one domain never matches the SID of an account or group in any other domain in the enterprise.

SIDs always remain unique. Security authorities never issue the same SID twice, and they never reuse SIDs for deleted accounts. For example, if a user with a user account in a Windows domain leaves their job, an administrator deletes their Active Directory account, including the SID that identifies the account. If they later return to a different job at the same company, an administrator creates a new account, and the Windows Server operating system generates a new SID. The new

SID doesn't match the old one, so none of the user's access from their old account is transferred to the new account. Both their accounts represent two different security principals.

SID architecture

A SID is a data structure in binary format that contains a variable number of values. The first values in the structure contain information about the SID structure. The remaining values are arranged in a hierarchy (similar to a telephone number), and they identify the SID-issuing authority (for example, NT Authority), the SID-issuing domain, and a particular security principal or group. The following image illustrates the structure of a SID.

 Diagram that shows the architecture of a security identifier and illustrates the domain identifier and relative identifier components.

The individual values of a SID are described in the following table:

Component	Description
Revision	Indicates the version of the SID structure that's used in a particular SID.
Identifier authority	Identifies the highest level of authority that can issue SIDs for a particular type of security principal. For example, the identifier authority value in the SID for the Everyone group is 1 (World Authority). The identifier authority value in the SID for a specific Windows Server account or group is 5 (NT Authority).
Subauthorities	Holds the most important information in a SID, which is contained in a series of one or more subauthority values. All values up to, but not including, the last value in the series collectively identify a domain in an enterprise. This part of the series is called the domain identifier. The last value in the series, the RID, identifies a particular account or group relative to a domain.

The components of a SID are easier to visualize when SIDs are converted from a binary to a string format by using standard notation:

```
S-R-X-Y1-Y2-Yn-1-Yn
```

In this notation, the components of a SID are described in the following table:

Component	Description
S	Indicates that the string is a SID
R	Indicates the revision level
X	Indicates the identifier authority value
Y	Represents a series of subauthority values, where *n* is the number of values

The SID's most important information is contained in the series of subauthority values. The first part of the series (-Y1-Y2-Y*n*-1) is the domain identifier. This element of the SID becomes significant in an enterprise with several domains. Specifically, the domain identifier differentiates SIDs that one domain issues from SIDs that all other domains in the enterprise issue. No two domains in an enterprise share the same domain identifier.

The last item in the series of subauthority values (-Y*n*) is the RID. It distinguishes one account or group from all other accounts and groups in the domain. No two accounts or groups in any domain share the same RID.

For example, the SID for the built-in Administrators group is represented in standardized SID notation as the following string:

S-1-5-32-544

This SID has four components:

- A revision level (1)
- An identifier authority value (5, NT Authority)

- A domain identifier (32, Builtin)
- An RID (544, Administrators)

SIDs for built-in accounts and groups always have the same domain identifier value, 32. This value identifies the domain, Builtin, which exists on every computer that's running a version of the Windows Server operating system. It's never necessary to distinguish one computer's built-in accounts and groups from another computer's built-in accounts and groups, because they're local in scope. They're local to a single computer or, with domain controllers for a network domain, they're local to several computers that are acting as one.

Built-in accounts and groups need to be distinguished from one another within the scope of the Builtin domain. Therefore, the SID for each account and group has a unique RID. An RID value of 544 is unique to the built-in Administrators group. No other account or group in the Builtin domain has a SID with a final value of 544.

In another example, consider the SID for the global group, Domain Admins. Every domain in an enterprise has a Domain Admins group, and the SID for each group is different. The following example represents the SID for the Domain Admins group in the Contoso, Ltd. domain (Contoso\Domain Admins):

S-1-5-21-1004336348-1177238915-682003330-512

The SID for Contoso\Domain Admins has the following components:

- A revision level (1)
- An identifier authority (5, NT Authority)
- A domain identifier (21-1004336348-1177238915-682003330, Contoso)
- An RID (512, Domain Admins)

The SID for Contoso\Domain Admins is distinguished from the SIDs for other Domain Admins groups in the same enterprise by its domain identifier: 21-1004336348-1177238915-682003330. No other domain in the enterprise uses this value as its domain identifier. The SID for Contoso\Domain Admins is distinguished from the SIDs for other accounts and groups that are created in the Contoso domain by its RID, 512. No other account or group in the domain has a SID with a final value of 512.

RID allocation

When accounts and groups are stored in an account database that a local Security Accounts Manager (SAM) manages, it's fairly easy for the system to generate a unique RID for each account and group that it creates on a standalone computer. The SAM on a standalone computer can track the RID values that it has used and make sure that it never uses them again.

In a network domain, however, generating unique RIDs is a more complex process. Windows Server network domains can have several domain controllers. Each domain controller stores Active Directory account information. As a result, in a network domain, there are as many copies of the account database as there are domain controllers. In addition, every copy of the account database is a master copy.

New accounts and groups can be created on any domain controller. Changes that are made to Active Directory on one domain controller are replicated to all other domain controllers in the domain. The process of replicating changes in one master copy of the account database to all other master copies is called a multimaster operation.

The process of generating unique RIDs is a single-master operation. One domain controller is assigned the role of RID master, and it allocates a sequence of RIDs to each domain controller in the domain. When a new domain account or group is created in one domain controller's replica of Active Directory, it's assigned a SID. The RID for the new SID is taken from the domain controller's allocation of RIDs. When its supply of RIDs begins to run low, the domain controller requests another block from the RID master.

Each domain controller uses each value in a block of RIDs only once. The RID master allocates each block of RID values only once. This process ensures that every account and group created in the domain has a unique RID.

SIDs and globally unique identifiers

When a new domain user or group account is created, Active Directory stores the account's SID in the `ObjectSID` property of a User or Group object. It also assigns the new object a globally unique identifier (GUID), which is a 128-bit value that's

unique not only in the enterprise, but also across the world. A GUID is assigned to every object that Active Directory creates, not only User and Group objects. Each object's GUID is stored in its `ObjectGUID` property.

Active Directory uses GUIDs internally to identify objects. For example, the GUID is one of an object's properties that's published in the global catalog. Searching the global catalog for a User object GUID produces results if the user has an account somewhere in the enterprise. In fact, searching for any object by `ObjectGUID` might be the most reliable way of finding the object you want to locate. The values of other object properties can change, but the `ObjectGUID` property never changes. When an object is assigned a GUID, it keeps that value for life.

If a user moves from one domain to another, the user gets a new SID. The SID for a Group object doesn't change, because groups stay in the domain where they're created. However, if people move, their accounts can move with them. If an employee moves from North America to Europe but stays in the same company, an administrator for the enterprise can move the employee's User object from, for example, Contoso\NoAm to Contoso\Europe. In this case, the User object for the account needs a new SID. The domain identifier portion of a SID that's issued in NoAm is unique to NoAm, so the SID for the user's account in Europe has a different domain identifier. The RID portion of a SID is unique relative to the domain, so if the domain changes, the RID also changes.

When a User object moves from one domain to another, a new SID must be generated for the user account and stored in the `ObjectSID` property. Before the new value is written to the property, the previous value is copied to another property of a User object, `SIDHistory`. This property can hold multiple values. Each time a User object moves to another domain, a new SID is generated and stored in the `ObjectSID` property, and another value is added to the list of old SIDs in the `SIDHistory` value. When a user signs in and is successfully authenticated, the domain authentication service queries Active Directory for all the SIDs that are associated with the user. The query includes the user's current SID, the user's old SIDs, and the SIDs for the user's groups. All these SIDs are returned to the authentication client, and they're included in the user's access token. When the user tries to gain access to a resource, any one of the SIDs in the access token (including one of the SIDs in the `SIDHistory` property), can allow or deny the user access.

You can allow or deny users access to a resource based on their jobs. But you should allow or deny access to a group, not to an individual. That way, when users change jobs or move to other departments, you can easily adjust their access by removing them from certain groups and adding them to others.

However, if you allow or deny an individual user access to resources, you probably want that user's access to remain the same no matter how many times the user's account domain changes. The `SIDHistory` property makes it possible for the access to remain the same. When a user changes domains, there's no need to change the access control list (ACL) on any resource. An ACL might have the user's old SID but not the new one. But the old SID is still in the user's access token. It's listed among the SIDs for the user's groups, and the user is granted or denied access based on the old SID.

Well-known SIDs

The values of certain SIDs are constant across all systems. They're created when the operating system or domain is installed. They're called well-known SIDs because they identify generic users or generic groups.

There are universal well-known SIDs that are meaningful on all secure systems that use this security model, including operating systems other than Windows. In addition, there are well-known SIDs that are meaningful only on Windows operating systems.

The following table lists the universal well-known SIDs:

Universal well-known SID	**Name**	**Identifies**
S-1-0-0	Null SID	A group with no members. This value is often used when a SID value isn't known.
S-1-1-0	World	A group that includes all users.
S-1-2-0	Local	Users who sign in to terminals that are locally (physically) connected to the system.
S-1-2-1	Console Logon	A group that includes users who are signed in to the physical console.

Universal well-known SID	Name	Identifies
S-1-3-0	Creator Owner ID	A SID to be replaced by the SID of the user who creates a new object. This SID is used in inheritable access control entries (ACEs).
S-1-3-1	Creator Group ID	A SID to be replaced by the primary-group SID of the user who creates a new object. Use this SID in inheritable ACEs.
S-1-3-2	Owner Server	A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the object's owner server and stores information about who created a given object or file.
S-1-3-3	Group Server	A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the object's group server. The system also stores information about the groups that are allowed to work with the object.
S-1-3-4	Owner Rights	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 standard access rights for the object owner.
S-1-4	Non-unique Authority	A SID that represents an identifier authority.
S-1-5	NT Authority	A SID that represents an identifier authority.
S-1-5-80-0	All Services	A group that includes all service processes configured on the system. The operating system controls the membership of this group.

The following table lists the predefined identifier authority constants. The first four values are used with universal well-known SIDs, and the rest of the values are used with well-known SIDs in the Windows operating systems in the "Applies to" list at the beginning of the article.

Identifier authority	Value	SID string prefix
SECURITY_NULL_SID_AUTHORITY	0	S-1-0
SECURITY_WORLD_SID_AUTHORITY	1	S-1-1
SECURITY_LOCAL_SID_AUTHORITY	2	S-1-2
SECURITY_CREATOR_SID_AUTHORITY	3	S-1-3
SECURITY_NT_AUTHORITY	5	S-1-5
SECURITY_AUTHENTICATION_AUTHORITY	18	S-1-18

The following RID values are used with universal well-known SIDs. The **Identifier authority** column shows the prefix of the identifier authority with which you can combine the RID to create a universal well-known SID.

RID authority	Value	Identifier authority
SECURITY_NULL_RID	0	S-1-0
SECURITY_WORLD_RID	0	S-1-1
SECURITY_LOCAL_RID	0	S-1-2
SECURITY_CREATOR_OWNER_RID	0	S-1-3
SECURITY_CREATOR_GROUP_RID	1	S-1-3

The SECURITY_NT_AUTHORITY (S-1-5) predefined identifier authority produces SIDs that aren't universal. These SIDs are meaningful only in installations of the Windows operating systems in the "Applies to" list at the beginning of this article.

The following table lists the well-known SIDs:

SID	Display name	Description
S-1-5-1	Dialup	A group that includes all users who are signed in to the system via dial-up connection.
S-1-5-113	Local account	A SID that you can use when you restrict network sign-in to local accounts instead of administrator or equivalent accounts. This SID can be effective in blocking network sign-in for local users and groups by account type regardless of their name.
S-1-5-114	Local account and member of Administrators group	A SID that you can use when you restrict network sign-in to local accounts instead of administrator or equivalent accounts. This SID can be effective in blocking network sign-in for local users and groups by account type regardless of their name.
S-1-5-2	Network	A group that includes all users who are signed in via a network connection. Access tokens for interactive users don't contain the Network SID.
S-1-5-3	Batch	A group that includes all users who are signed in via batch queue facility, such as task scheduler jobs.
S-1-5-4	Interactive	A group that includes all users who sign in interactively. A user can start an interactive sign-in session by opening a Remote Desktop Services connection from a remote computer, or by using a remote shell such as Telnet. In each case, the user's access token contains the Interactive SID. If the user signs in by using a Remote Desktop Services connection, the user's access token also contains the Remote Interactive Logon SID.
S-1-5-5- *X*-*Y*	Logon Session	A particular sign-in session. The *X* and *Y* values for SIDs in this format are unique for each sign-in session.
S-1-5-6	Service	A group that includes all security principals that are signed in as a service.
S-1-5-7	Anonymous Logon	A user who connects to the computer without supplying a user name and password. The Anonymous Logon identity is different from the identity that's used by Internet Information Services (IIS) for anonymous web access. IIS uses an actual account—by default, IUSR_*computer-name*, for anonymous access to resources on a website. Strictly speaking, such access isn't anonymous, because the security principal is known even though unidentified people are using the account. IUSR_*computer-name* (or whatever you name the account) has a password, and IIS signs in to the account when the service starts. As a result, the IIS anonymous user is a member of Authenticated Users, but Anonymous Logon isn't.
S-1-5-8	Proxy	A SID that's not currently used.
S-1-5-9	Enterprise Domain Controllers	A group that includes all domain controllers in a forest of domains.
S-1-5-10	Self	A placeholder in an ACE for a user, group, or computer object in Active Directory. When you grant permissions to Self, you grant them to the security principal that the object represents. During an access check, the operating system replaces the SID for Self with the SID for the security principal that the object represents.

SID	Display name	Description
S-1-5-11	Authenticated Users	A group that includes all users and computers with identities that have been authenticated. Authenticated Users doesn't include the Guest account even if that account has a password. This group includes authenticated security principals from any trusted domain, not only the current domain.

S-1-5-12	Restricted Code	An identity that's used by a process that's running in a restricted security context. In Windows and Windows Server operating systems, a software restriction policy can assign one of three security levels to code:
		`Unrestricted`
		`Restricted`
		`Disallowed`
		When code runs at the restricted security level, the Restricted SID is added to the user's access token.

S-1-5-13	Terminal Server User	A group that includes all users who sign in to a server with Remote Desktop Services enabled.
S-1-5-14	Remote Interactive Logon	A group that includes all users who sign in to the computer by using a remote desktop connection. This group is a subset of the Interactive group. Access tokens that contain the Remote Interactive Logon SID also contain the Interactive SID.
S-1-5-15	This Organization	A group that includes all users from the same organization. This group is included only with Active Directory accounts and added only by a domain controller.
S-1-5-17	IUSR	An account that's used by the default IIS user.
S-1-5-18	System (or LocalSystem)	An identity that's used locally by the operating system and by services that are configured to sign in as LocalSystem. System is a hidden member of Administrators. That is, any process that's running as System has the SID for the built-in Administrators group in its access token. When a process that's running locally as System accesses network resources, it does so by using the computer's domain identity. Its access token on the remote computer includes the SID for the local computer's domain account plus SIDs for security groups that the computer is a member of, such as Domain Computers and Authenticated Users.
S-1-5-19	NT Authority (LocalService)	An identity that's used by services that are local to the computer, have no need for extensive local access, and don't need authenticated network access. Services that run as LocalService can access local resources as ordinary users, and they access network resources as anonymous users. As a result, a service that runs as LocalService has significantly less authority than a service that runs as LocalSystem locally and on the network.
S-1-5-20	NetworkService	An identity that's used by services that have no need for extensive local access but do need authenticated network access. Services that are running as NetworkService can access local resources as ordinary users and access network resources by using the computer's identity. As a result, a service that runs as NetworkService has the same network access as a service that runs as LocalSystem, but its local access is significantly reduced.
S-1-5-*domain*-500	Administrator	A user account for the system administrator. Every computer has a local Administrator account, and every domain has a domain Administrator account. The Administrator account is the first account created during operating

SID	Display name	Description
		system installation. The account can't be deleted, disabled, or locked out, but it can be renamed. By default, the Administrator account is a member of the Administrators group, and it can't be removed from that group.
S-1-5-*domain*-501	Guest	A user account for people who don't have individual accounts. Every computer has a local Guest account, and every domain has a domain Guest account. By default, Guest is a member of the Everyone and the Guests groups. The domain Guest account is also a member of the Domain Guests and Domain Users groups. Unlike Anonymous Logon, Guest is a real account, and it can be used to sign in interactively. The Guest account doesn't require a password, but it can have one.
S-1-5-*domain*-502	KRBTGT	A user account that's used by the Key Distribution Center (KDC) service. The account exists only on domain controllers.
S-1-5-*domain*-512	Domain Admins	A global group with members that are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that are joined to the domain, including domain controllers. Domain Admins is the default owner of any object that's created in the domain's Active Directory by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.
S-1-5-*domain*-513	Domain Users	A global group that includes all users in a domain. When you create a new User object in Active Directory, the user is automatically added to this group.
S-1-5-*domain*-514	Domain Guests	A global group that, by default, has only one member: the domain's built-in Guest account.
S-1-5-*domain*-515	Domain Computers	A global group that includes all computers that are joined to the domain, excluding domain controllers.
S-1-5-*domain*-516	Domain Controllers	A global group that includes all domain controllers in the domain. New domain controllers are added to this group automatically.
S-1-5-*domain*-517	Cert Publishers	A global group that includes all computers that host an enterprise certification authority. Cert Publishers are authorized to publish certificates for User objects in Active Directory.
S-1-5-*root domain*-518	Schema Admins	A group that exists only in the forest root domain. It's a universal group if the domain is in native mode, and it's a global group if the domain is in mixed mode. The Schema Admins 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.
S-1-5-*root domain*-519	Enterprise Admins	A group that exists only in the forest root domain. It's a universal group if the domain is in native mode, and it's a global group if the domain is in mixed mode. The Enterprise Admins group is authorized to make changes to the forest infrastructure. Examples include adding child domains, configuring sites, authorizing Dynamic Host Configuration Protocol (DHCP) servers, and installing enterprise certification authorities. By default, the only member of Enterprise Admins is the Administrator

SID	Display name	Description
		account for the forest root domain. The group is a default member of every Domain Admins group in the forest.
S-1-5-*domain*-520	Group Policy Creator Owners	A global group that's authorized to create new Group Policy Objects in Active Directory. By default, the only member of the group is Administrator. When a member of Group Policy Creator Owners creates an object, that member owns the object. In this way, the Group Policy Creator Owners group is unlike other administrative groups (such as Administrators and Domain Admins). When a member of these groups creates an object, the group owns the object, not the individual.
S-1-5-*domain*-521	Read-only Domain Controllers	A global group that includes all read-only domain controllers.
S-1-5-*domain*-522	Clonable Controllers	A global group that includes all domain controllers in the domain that can be cloned.
S-1-5-*domain*-525	Protected Users	A global group that's afforded extra protections against authentication security threats.
S-1-5-*root domain*-526	Key Admins	A group that's intended for use in scenarios where trusted external authorities are responsible for modifying this attribute. Only trusted administrators should be made a member of this group.
S-1-5-*domain*-527	Enterprise Key Admins	A group that's intended for use in scenarios where trusted external authorities are responsible for modifying this attribute. Only trusted enterprise administrators should be made a member of this group.
S-1-5-32-544	Administrators	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.
S-1-5-32-545	Users	A built-in group. After the initial installation of the operating system, the only member is the Authenticated Users group.
S-1-5-32-546	Guests	A built-in group. By default, the only member is the Guest account. The Guests group allows occasional or one-time users to sign in with limited privileges to a computer's built-in Guest account.
S-1-5-32-547	Power Users	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 create. • Remove users from the Power Users, Users, and Guests groups. • Install programs. • Create, manage, and delete local printers. • Create and delete file shares.
S-1-5-32-548	Account Operators	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 (OUs) of Active Directory except the Builtin container and the Domain Controllers OU. Account Operators don't have permission to modify the Administrators and Domain Admins groups. They also don't have permission to modify the accounts for members of those groups.

SID	Display name	Description
S-1-5-32-549	Server Operators	A built-in group that exists only on domain controllers. By default, the group has no members. Server Operators can: • Sign in 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. • Shut down the computer.
S-1-5-32-550	Print Operators	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.
S-1-5-32-551	Backup Operators	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 sign in to the computer and shut it down.
S-1-5-32-552	Replicators	A built-in group that supports file replication in a domain. By default, the group has no members. *Don't* add users to this group.
S-1-5-*domain*-553	RAS and IAS Servers	A local domain group. By default, this group has no members. Computers that are running the Routing and Remote Access Service are added to the group automatically. Members of this group have access to certain properties of User objects, such as Read Account Restrictions, Read Logon Information, and Read Remote Access Information.
S-1-5-32-554	Builtin\Pre-Windows 2000 Compatible Access	A backward compatibility group that allows read access on all users and groups in the domain.
S-1-5-32-555	Builtin\Remote Desktop Users	An alias. Members of this group are granted the right to sign in remotely.
S-1-5-32-556	Builtin\Network Configuration Operators	An alias. Members of this group can have some administrative privileges to manage configuration of networking features.
S-1-5-32-557	Builtin\Incoming Forest Trust Builders	An alias. Members of this group can create incoming, one-way trusts to the forest.
S-1-5-32-558	Builtin\Performance Monitor Users	An alias. Members of this group have remote access to monitor the computer.
S-1-5-32-559	Builtin\Performance Log Users	An alias. Members of this group have remote access to schedule logging of performance counters on the computer.
S-1-5-32-560	Builtin\Windows Authorization Access Group	An alias. Members of this group have access to the computed `tokenGroupsGlobalAndUniversal` attribute on User objects.
S-1-5-32-561	Builtin\Terminal Server License Servers	An alias. A group for Terminal Server license servers.
S-1-5-32-562	Builtin\Distributed COM Users	An alias. A group for Component Object Model (COM) users to provide computer-wide access controls that govern access to all call, activation, or launch requests on the computer.

SID	Display name	Description
S-1-5-32-568	Builtin\IIS_IUSRS	An alias. A built-in group account for IIS users.
S-1-5-32-569	Builtin\Cryptographic Operators	A built-in local group. Members are authorized to perform cryptographic operations.
S-1-5-*domain*-571	Allowed RODC Password Replication Group	A group with members who can have their passwords replicated to all read-only domain controllers in the domain.
S-1-5-*domain*-572	Denied RODC Password Replication Group	A group with members who can't have their passwords replicated to all read-only domain controllers in the domain.
S-1-5-32-573	Builtin\Event Log Readers	A built-in local group. Members of this group can read event logs from a local computer.
S-1-5-32-574	Builtin\Certificate Service DCOM Access	A built-in local group. Members of this group are allowed to connect to certification authorities in the enterprise.
S-1-5-32-575	Builtin\RDS Remote Access Servers	A built-in local group. Servers in this group give users of RemoteApp programs and personal virtual desktops access to these resources. In internet-facing deployments, these servers are typically deployed in an edge network. This group needs to be populated on servers that are running Remote Desktop Connection Broker (RD Connection Broker). Remote Desktop Gateway (RD Gateway) servers and Remote Desktop Web Access (RD Web Access) servers used in the deployment need to be in this group.
S-1-5-32-576	Builtin\RDS Endpoint Servers	A built-in local group. Servers in this group run virtual machines and host sessions where users' RemoteApp programs and personal virtual desktops run. This group needs to be populated on servers that are running RD Connection Broker. Remote Desktop Session Host (RD Session Host) servers and Remote Desktop Virtualization Host (RD Virtualization Host) servers used in the deployment need to be in this group.
S-1-5-32-577	Builtin\RDS Management Servers	A built-in local group. Servers in this group can perform routine administrative actions on servers that are running Remote Desktop Services. This group needs to be populated on all servers in a Remote Desktop Services deployment. The servers that are running the Remote Desktop Services central management service must be included in this group.
S-1-5-32-578	Builtin\Hyper-V Administrators	A built-in local group. Members of this group have complete and unrestricted access to all features of Hyper-V.
S-1-5-32-579	Builtin\Access Control Assistance Operators	A built-in local group. Members of this group can remotely query authorization attributes and permissions for resources on the computer.
S-1-5-32-580	Builtin\Remote Management Users	A built-in local group. Members of this group can access Windows Management Instrumentation (WMI) resources over management protocols such as Web Services for Management (WS-Management) via the Windows Remote Management service. This access applies only to WMI namespaces that grant access to the user.
S-1-5-64-10	NTLM Authentication	A SID that's used when the New Technology LAN Manager (NTLM) authentication package authenticates the client.
S-1-5-64-14	SChannel Authentication	A SID that's used when the Secure Channel (Schannel) authentication package authenticates the client.

SID	Display name	Description
S-1-5-64-21	Digest Authentication	A SID that's used when the Digest authentication package authenticates the client.
S-1-5-80	NT Service	A SID that's used as a New Technology Service (NT Service) account prefix.
S-1-5-80-0	All Services	A group that includes all service processes that are configured on the system. The operating system controls the membership of this group. The S-1-5-80-0 SID represents NT SERVICES\ALL SERVICES.
S-1-5-83-0	NT VIRTUAL MACHINE\Virtual Machines	A built-in group. The group is created when the Hyper-V role is installed. The Hyper-V Management Service (VMMS) maintains the membership of this group. This group requires the *Create Symbolic Links* right (SeCreateSymbolicLinkPrivilege) and the *Log on as a Service* right (SeServiceLogonRight).

The following RIDs are relative to each domain:

RID	Decimal value	Identifies
DOMAIN_USER_RID_ADMIN	500	The administrative user account in a domain.
DOMAIN_USER_RID_GUEST	501	The guest-user account in a domain. Users who don't have an account can automatically sign in to this account.
DOMAIN_GROUP_RID_USERS	513	A group that contains all user accounts in a domain. All users are automatically added to this group.
DOMAIN_GROUP_RID_GUESTS	514	The group Guest account in a domain.
DOMAIN_GROUP_RID_COMPUTERS	515	The Domain Computer group. All computers in the domain are members of this group.
DOMAIN_GROUP_RID_CONTROLLERS	516	The Domain Controller group. All domain controllers in the domain are members of this group.
DOMAIN_GROUP_RID_CERT_ADMINS	517	The certificate publishers group. Computers that are running Active Directory Certificate Services are members of this group.
DOMAIN_GROUP_RID_SCHEMA_ADMINS	518	The schema administrators group. Members of this group can modify the Active Directory schema.
DOMAIN_GROUP_RID_ENTERPRISE_ADMINS	519	The enterprise administrators group. Members of this group have full access to all domains in the Active Directory forest. Enterprise administrators are responsible for forest-level operations such as adding or removing new domains.
DOMAIN_GROUP_RID_POLICY_ADMINS	520	The policy administrators group.

The following table lists examples of domain-relative RIDs that are used to form well-known SIDs for local groups:

RID	Decimal value	Identifies
DOMAIN_ALIAS_RID_ADMINS	544	Administrators of the domain.
DOMAIN_ALIAS_RID_USERS	545	All users in the domain.
DOMAIN_ALIAS_RID_GUESTS	546	Guests of the domain.
DOMAIN_ALIAS_RID_POWER_USERS	547	A user or a set of users who expect to treat a system as if it were their personal computer rather than as a workstation for multiple users.
DOMAIN_ALIAS_RID_BACKUP_OPS	551	A local group that's used to control the assignment of file backup-and-restore user rights.
DOMAIN_ALIAS_RID_REPLICATOR	552	A local group that's responsible for copying security databases from the primary domain controller to the backup domain controllers. These accounts are used only by the system.
DOMAIN_ALIAS_RID_RAS_SERVERS	553	A local group that represents remote access and servers that are running Internet Authentication Service (IAS). This group permits access to various attributes of User objects.

Changes in SID functionality

The following table describes changes in SID implementation in the Windows operating systems:

Change	Operating system version	Description and resources
The TrustedInstaller SID owns most of the operating system files	Windows Server 2008, Windows Vista	The purpose of this change is to prevent a process that's running as an administrator or under the LocalSystem account from automatically replacing the operating system files.
Restricted SID checks are implemented	Windows Server 2008, Windows Vista	When restricting SIDs are present, Windows performs two access checks. The first is the normal access check, and the second is the same access check against the restricting SIDs in the token. Both access checks must pass to allow the process to access the object.

Capability SIDs

Capability SIDs serve as unique and immutable identifiers for capabilities. A capability represents an unforgeable token of authority that grants Universal Windows Applications access to resources (for example, documents, cameras, and locations). An app that *has* a capability is granted access to the resource that the capability is associated with. An app that *doesn't have* a capability is denied access to the resource.

All capability SIDs that the operating system is aware of are stored in the Windows registry in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities path. Any capability SID that's added to Windows by Microsoft or partner applications is added to this location.

Examples of registry keys taken from Windows 10, version 1909, 64-bit Enterprise edition

You might see the following registry keys under AllCachedCapabilities:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_DevU
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_DevU
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_Enter

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_Gener
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_Restri
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_Wind

The prefix of all capability SIDs is S-1-15-3.

Examples of registry keys taken from Windows 11, version 21H2, 64-bit Enterprise edition

You might see the following registry keys under AllCachedCapabilities:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_DevU
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_DevU
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_Enter
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_Gener
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_Restri
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities\capabilityClass_Wind

The prefix of all capability SIDs is S-1-15-3.

Related content

- Access control overview
