DEFINITION

security identifier (SID)

Peter Loshin, Former Senior Technology Editor

What is a security identifier (SID)?

In the context of Windows computing and Microsoft Active Directory (AD), a security identifier (SID) is a unique value that is used to identify any security entity that the Windows operating system (OS) can authenticate. A security entity can be a security principal -- a user account, a computer account or a process started by those accounts -- or it can be a security group.

All Windows objects that can be uniquely identified by name store their SID, along with any discretionary access control lists and system ACLs, in a security descriptor data structure.

How do SIDs work?

Microsoft Windows security depends on SIDs for authentication. Windows server OSes use SIDs to uniquely identify accounts on the local computer in a persistent way: A user account name could change, but since the SID stays the same, that account can still be identified.

When a computer joins a domain, the domain controller grants it a Domain SID for authentication purposes in the domain. ACLs include lists of SIDs for security principals and groups that are authorized for access to that domain.

There are also well-known SIDs, which are identifiers for generic groups and users that are valid and persistent on all Windows systems. For example, two commonly used well-known SIDs specify the all users group or the Null SID, which is a group that has no members.

Why are SIDs used?

SIDs are used as a unique identifier for entities that use Windows. SIDs are a component of a security database that security authorities can use to identify the user and the permissions that user is entitled to.

When users log on to a Windows system, the system generates an access token that includes the user SID, the SID of any groups the user belongs to and the user privilege level. This access token can be authenticated against an ACL to determine what the user can access.

What is the format of SIDs?

A SID is a data structure that organizes SID information in a logical structure consisting of values, including the following:

- **Revision** is the version level of the SID and is required to be initialized as 0x01.
- **SubAuthorityCount** is the number of subauthorities in the SID.
- **IdentifierAuthority** is the entity that created the SID, usually represented as three 16-bit numbers separated by hyphens.
- **SubAuthority** is a component of the SID's domain, and an SID may include up to 15 subauthorities, each of which is identified by a 32-bit subauthority value.

The SID structure is stored as binary data and converted to a string format for reading. Basic syntax rules for SIDs include the following:

- All SIDs start with the letter "S."
- Individual components of the SID are separated by hyphens.
- Individual components of the SID are strings composed of numbers and hyphens.
- SIDs are composed of four components:
    - revision level
    - identifier authority
    - domain identifier
    - relative identifier

A typical SID looks like this:

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

This SID is the unique identifier for Microsoft's example domain for the Domain Admins group at Contoso Ltd. Contoso is a fictional company often used as an example for Microsoft domains. This SID consists of four discrete components in addition to the "S-" prefix that identifies it as an SID. The other components are the following:

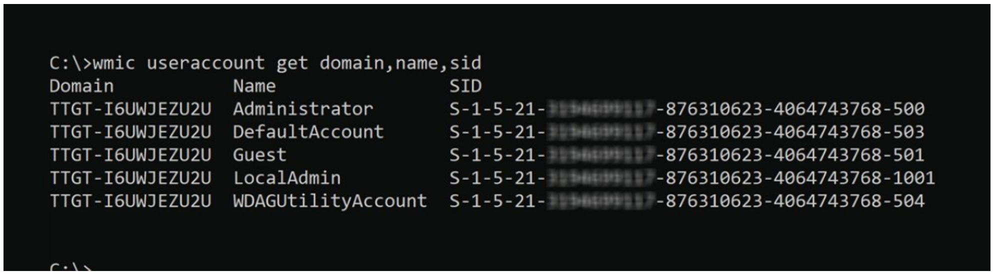
- **1** indicates the revision level.
- **5** is the identifier authority, indicating the NT authority; this value is only used for Microsoft Windows installations. Valid values are 0 through 5, indicating the following:
  - 0 null authority
  - 1 world authority
  - 2 local authority
  - 3 creator authority
  - 4 nonunique authority
  - 5 NT authority
- **21-1004336348-1177238915-682003330** is the domain identifier that uniquely identifies Contoso as the domain.
- **512** is the relative ID specifying the Domain Admins group within the Contoso domain.

How to find a SID number

SIDs are stored in the Windows registry and can be found using Windows Registry Editor. To discover SIDs using the Windows command prompt, enter the following command:

```
wmic useraccount get domain,name,sid
```

WMIC stands for Windows Management Instrumentation Command, a software utility that enables users to perform Windows administration tasks through the command line.



```
C:\>wmic useraccount get domain,name,sid
Domain           Name                SID
TTGT-I6UWJEZU2U  Administrator       S-1-5-21-[redacted]-876310623-4064743768-500
TTGT-I6UWJEZU2U  DefaultAccount      S-1-5-21-[redacted]-876310623-4064743768-503
TTGT-I6UWJEZU2U  Guest               S-1-5-21-[redacted]-876310623-4064743768-501
TTGT-I6UWJEZU2U  LocalAdmin          S-1-5-21-[redacted]-876310623-4064743768-1001
TTGT-I6UWJEZU2U  WDAGUtilityAccount  S-1-5-21-[redacted]-876310623-4064743768-504

C:\>
```

Using wmic (Windows Management Instrumentation Command) to retrieve SIDs for Windows

To get the SID for the current logged-in user from the command prompt, enter the following command:

```
whoami /user
```

whoami retrieves SID for Windows user

Using the whoami command to retrieve the SID for the current Windows user

SID is just one component of many in the Microsoft AD security infrastructure. Take this quiz to test your AD knowledge, or read on to learn more about techniques for troubleshooting AD issues.

This was last updated in March 2022

Continue Reading About security identifier (SID)