How can I force a user to have a specific SID prefix, so that they go into a particular group?

devblogs.microsoft.com/oldnewthing/20230105-00

January 5, 2023

Raymond Chen

A customer wanted to create a user with a specific SID prefix:

> We know that you can’t create a user with a specific SID, but can we at least create it with a specific SID prefix?
>
> We naïvely tried this:
>
> ```
> net user /add Fred
> net localgroup "Cryptographic Operators" Fred /add
> ```
>
> Since the Cryptographic Operators group SID is S-1-5-32-569, we expected that the newly-created user “Fred” would have a SID of the form S-1-5-32-569-(random)-1000, but it doesn’t.
>
> How do we create a user with a specific SID prefix? We want Fred to be a member of the “Cryptographic Operators” group, so we need the user SID to be under the “Cryptographic Operators” SID.

Okay, that’s not how SID prefixes work.

Group membership is not controlled by SID prefixes. It is not the case that all members of the “Cryptographic Operators” group have a SID prefix of S-1-5-32-569, nor is it the case that you must have that prefix in order to be a member of the “Cryptographic Operators” group.

In fact, S-1-5-32-569 is not a legal SID prefix at all, since it is not a so-called *domain identifier*, which is the fancy name for “a thing that can produce new SIDs via suffixing.”

If you think about it, it makes sense that group membership is not controlled by SID prefixes. After all, a user can belong to multiple groups: You are probably a member of the local Administrators group (S-1-5-32-544), the Remote Desktop Users group (S-1-5-32-555), the Users group (S-1-5-32-545), the Authenticated Users group (S-1-5-11), and a whole bunch of others. But you have only one SID, so it can’t have all of those groups as a prefix.

Group membership is determined by entries in the user's token, and those entries are placed there at token creation based on the group memberships. When the system later wants to check if a user is in a group, it does so by looking in the token to see if there is an entry for that group in the token. It doesn't do it by doing a prefix check on the user SID.

You have your gym membership card in your wallet, but that doesn't mean that you were born at the gym. Your national identity number was issued by Stockholm, but that doesn't prevent you from being a registered resident of Göteborg.

The way to create a user in a group is to do exactly what the customer did: Create the user (which will assign them a SID), and then add the user to the groups you want them to be members of (which will add them in the group membership database).

The numeric properties of the SID are not important. As long as each entity gets a unique SID, that's the important thing. The prefixing technique is just a way to make sure that separate SID-creating entities can create unique SIDs without colliding with each other: If you give each SID-creating entity a unique prefix to stamp onto its created SIDs, then you can be sure that their SIDs won't collide.

Bonus chatter: Although the numeric properties are not important from a security standpoint, you can use knowledge of the SID-assignment algorithm to infer information about the circumstances of the SID's creation, in the same way that looking at a person's national identity number tells you where they were born.[1] For example, by looking at the SID, you can determine which SID-creating entity issued it, and from the RID you can infer which domain controller was used.

[1] In 1990, Sweden stopped encoding geographic information in the national identity number, so that trick works only for older people.