

# SID Nedir? SID Numarası & Security Identifiers

**MUSTAFA SERHAT DÜNDAR, <SERHAT AT SERHATDUNDAR DOT COM>, 21/06/2009**

## SID NEDİR?

Microsoft işletim sistemlerinin kurulduğu her bilgisayar kendisine ait karakteristiği taşıyan özel bir güvenlik tanımlayıcısı oluşturur. Bu güvenlik tanımlayıcısı ilerleyen zamanlarda yine bu bilgisayara ait görev ve yetkilerin kimliği görevini üstlenecektir. Domaine dahil edilmiş bir işletim sistemi üzerinde ki SID o makinenin fiziksel tanımlayıcılarını kullanarak kendini belirleyen özel bir Hex yapısı oluşturur. Sadece küçük bir hex yapısı o bilgisayara ait bütün özellik ve öğeleri Servera gösterebilir. Bu görevlendirme ve yetki alanları server harici lokasyon edilmiş ağlarda da geçerlidir.

## SID NE İÇERİR ?

\*Bilgisayar Adı

\*Varsa dahil olduğu Server yapısının özellikleri

\*Ağ tümleşik ve mekanik parçalarının fiziksel ( mac ) adresleri

\*İşletim sisteminin spesifik özellikleri ( version , Patch vs. )

\*Yetki ve Etki alanlarındaki Permission düzeyi

Kullanıcı, bilgisayar ve grup hesapları oluşturulduklarında, bu hesaplara otomatik olarak SID(security identifier) isimli bir numara atanır. SID oluşturulan hesabı tanımlayan benzersiz bir numaradır. SID NT4.0 zamanından bu yana hala kullanılmaktadır. Sistem hiçbir zaman sizi isminizle bilmez, SID numaranızla bilir ve tanır. Kullanıcı isimleri sadece bizim grafiksel arayüzden verdiğimiz tanımlamalardır. Bir kullanıcı adını silip, tekrar aynı adla yeni bir kullanıcı açmak grafiksel arayüzden mümkündür. Fakat isimleri aynı olmasına rağmen iki kullanıcıların SID numaraları hiçbir zaman arka planda aynı olmaz. Çünkü SID hiçbir zaman tekrar kullanılmaz. Kullanıcı hesabı silindiği anda SID numarası da onunla birlikte silinir. Tipik bir SID örneğini aşağıda görmekteyiz.

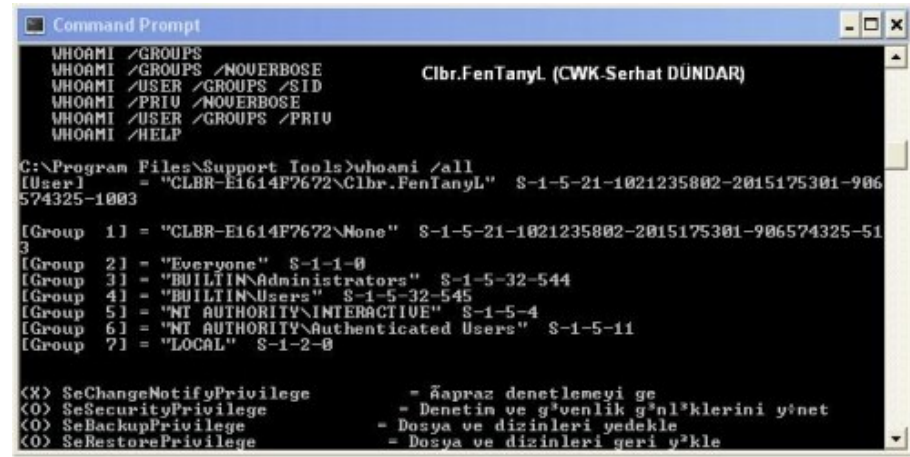
S-1-5-21-1659004503-193565697-854245398-1002

SID numarasını farklı segmentlere bölebilirsiniz. Örneğin aşağıdaki gibi :

#### S-1-5-21-D1-D2-D3-RID

S-1-5 standart bir ön ektir. Burada 1 versiyon numarasıdır ve NT 3.1 versiyondan bu yana hiç değışmedi. 5 ise SID'nin NT tarafından atandığını gösteren tanımlamadır. 21 yine bir NT ön ektir. D1,D2,D3 ise domain'e özgü olan 32-bitlik tanımlayıcı numaradır. Bir domain kurulunca D1'den D3'e kadar olan numara otomatik oluşur ve aynı domain içerisindeki bütün objeler için bu D1,D2,D3 değerleri aynı olur. En sondaki RID, relative identifier'ın kısaltmasıdır. Ve SID numarası içerisinde ait olduğu objeyi benzersiz kılan ve diğer objelerden ayıran numaradır. Her yeni hesap benzersiz bir RID numarasına sahiptir. Hatta eski kullanıcı ile aynı isim ve bilgiler kullanılsa bile RID her zaman farklıdır. Dolayısıyla, yeni açılan kullanıcının adı eski kullanıcı ile aynı olsa da RID numarası farklı olacağı için eski kullanıcının haklarını hiçbir şekilde kullanamayacaktır.

## WINDOWS SUPPORT TOOLS / WHOAMI



```
Command Prompt
WHOAMI /GROUPS
WHOAMI /GROUPS /NOVERBOSE
WHOAMI /USER /GROUPS /SID
WHOAMI /PRIV /NOVERBOSE
WHOAMI /USER /GROUPS /PRIV
WHOAMI /HELP

C:\Program Files\Support Tools>whoami /all
[User] = "CLBR-E1614F7672\Clbr.FenTanyL" S-1-5-21-1021235802-2015175301-906574325-1003

[Group 1] = "CLBR-E1614F7672\None" S-1-5-21-1021235802-2015175301-906574325-513
[Group 2] = "Everyone" S-1-1-0
[Group 3] = "BUILTIN\Administrators" S-1-5-32-544
[Group 4] = "BUILTIN\Users" S-1-5-32-545
[Group 5] = "NT AUTHORITY\INTERACTIVE" S-1-5-4
[Group 6] = "NT AUTHORITY\Authenticated Users" S-1-5-11
[Group 7] = "LOCAL" S-1-2-0

<X> SeChangeNotifyPrivilege = Ėapraz denetlemeyi ge
<O> SeSecurityPrivilege = Denetim ve g'venlik g'nll'klerini y'net
<O> SeBackupPrivilege = Dosya ve dizinleri yedekle
<O> SeRestorePrivilege = Dosya ve dizinleri geri y'kle
```

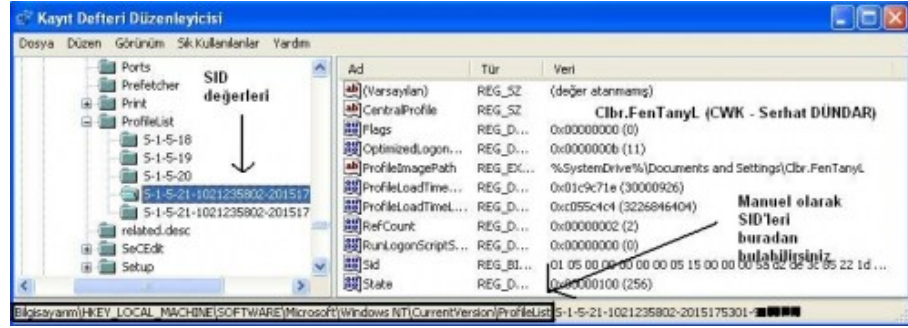
Whoami ile kullanıcıların ve grupların SID değerlerini görebilirsiniz.

Command Prompt'taki örnek kullanım :

whoami / all

whoami /groups / SID

Manuel olarak ise regeditten SID değerlerini bulabilirsiniz.



## SID DEĞERİNİ DEĞİŞTİRMEK

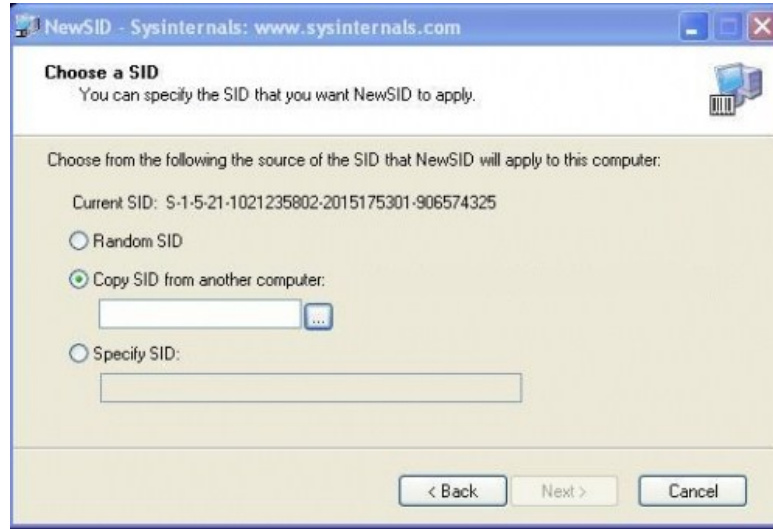
<http://technet.microsoft.com/en-us/sysinternals/bb897418.aspx> adresinden indirebileceğiniz newSID isimli yazılımla SID değerini değiştirebilirsiniz.

3 seçeneği olan bu yazılımla :

- 1) Herhangi bir değerle şuan ki SID değerini değiştirebilir.
- 2) Başka bir bilgisayarın SID değerini kendinize kopyalayabilir.
- 3) Kendi belirlediğiniz bir SID değeri oluşturabilirsiniz.

## UYARILAR !

- SID değerinin tüm sistemde değişmesi sistem özelliklerinize bağlı olarak 10-20 dakika arasında zaman alabilir.
- İşlemden önce bilgisayarınızın yedeğini alınız.
- Bu işlem sırasında yeni bir uygulama çalıştırmayınız.
- İşlemi iptal etmeye çalışmayınız.
- İşlemin sorunla karşılaşması, kesilmesi, aksaması Windows'unuzun çökmesine, kararsız işlemler yürütmesine sebep olacaktır.
- Tüm işlemler bitince bilgisayarınızı yeniden başlatınız.



## TAVSİYE BAĞLANTILAR & KAYNAKÇA :

<http://www.linglom.com/2007/12/14/sid-issue-of-duplicated-windows-virtual-disk/>

<http://support.microsoft.com/kb/243330>

[http://en.wikipedia.org/wiki/Relative\\_ID](http://en.wikipedia.org/wiki/Relative_ID)

[http://en.wikipedia.org/wiki/Security\\_Identifier](http://en.wikipedia.org/wiki/Security_Identifier)

<http://servermigrator.blogspot.com/2006/02/why-understanding-sids-is-important.html>

<http://sistemcini.com/sid-security-identifier-nedir/>