

## Windows 7 - Whoami

Bei Windows 8/7 und Vista ist die Benutzerverwaltung, die zentrale Stelle zur Verwaltung der angelegten Benutzer. Wer weitere Informationen zu einem Benutzer erfahren möchte, der nutzt den **DOS Befehl „whoami“**.

Whoami liefert Informationen wie z.B. die **SID, Anmelde-ID** eines Users, sowie Gruppenzuordnungen, Berechtigungen und Attribute.

Folgende Möglichkeiten bringt der Befehl zur Ausführung mit:

**/upn** Zeigt Benutzernamen und Benutzerprinzipalnamen (UPN-Format) an.

**/fqdn** Zeigt Benutzernamen mit dem vollständig qualifizierten Domännennamen(FQDNFormat) an.

**/user** Zeigt Informationen über den Benutzer mit der Sicherheitskennung (SID) an.

**/groups** Zeigt die Gruppenmitgliedschaft, die Sicherheitskennungen (SID) und Attribute an.

**/priv** Zeigt die Berechtigungen des Benutzers an.

**/logonid** Zeigt die Anmeldekennung des Benutzers an.

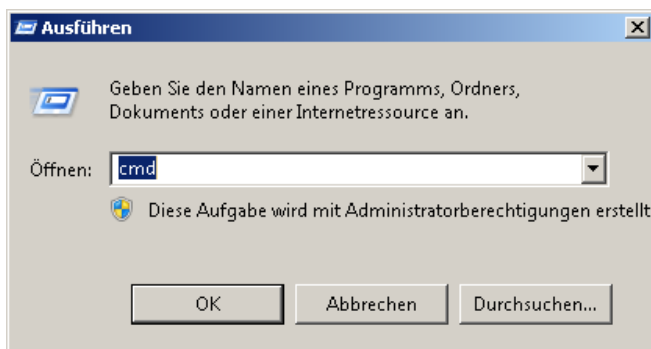
**/all** Zeigt den Benutzernamen, Gruppenmitgliedschaften mit den Sicherheitskennungen (SID) und Berechtigungen für das aktuelle Benutzerzugriffstoken an.

**/fo format** Bestimmt das Ausgabeformat: Gültige Werte: TABLE,LIST oder CSV. Spaltenheader werden nicht im CSV-Format angezeigt. Standardformat: TABLE.

**/nh** Legt fest, dass der Spaltenheader nicht in der Ausgabe angezeigt wird. Gilt nur für die Formate TABLE und CSV.

**/?** Zeigt Hilfe an

Wir öffnen das Kommandozeilen Tool über Start > Ausführen und dem Befehl CMD.



Eine SID ist ein Sicherheits-Identifikator der automatisch vom System vergeben wird. Anhand dieser SID werden z.B. Systeme, Benutzer und Gruppen identifiziert. Gruppen wie die Administratoren bekommen immer die gleiche SID, damit sie auf allen Systemen wieder zu finden sind. Erleichtert das globale Management!

## Windows 7 - Whoami

### Wie ist eine SID aufgebaut?

Die **SID** besteht aus 5 zusammenhängenden Teilen:

**S** – steht für SID

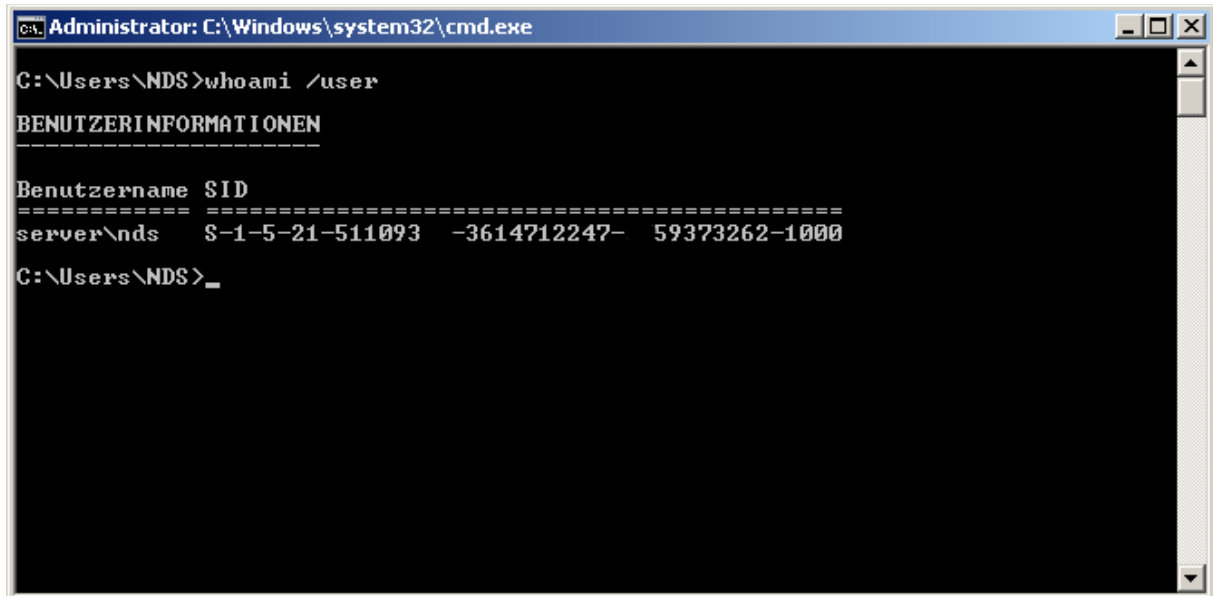
**1** – für Revisionsnummer

**5** – Identifier Authority

**21-51109305-3614712247-3759373262** steht für eine Domäne oder lokales System

**1000** – ist die Benutzernummer; diese beginnt bei 1000 und wird laufend hochgezählt

Die eigene SID erfahren wir über die Syntax `whoami /user`



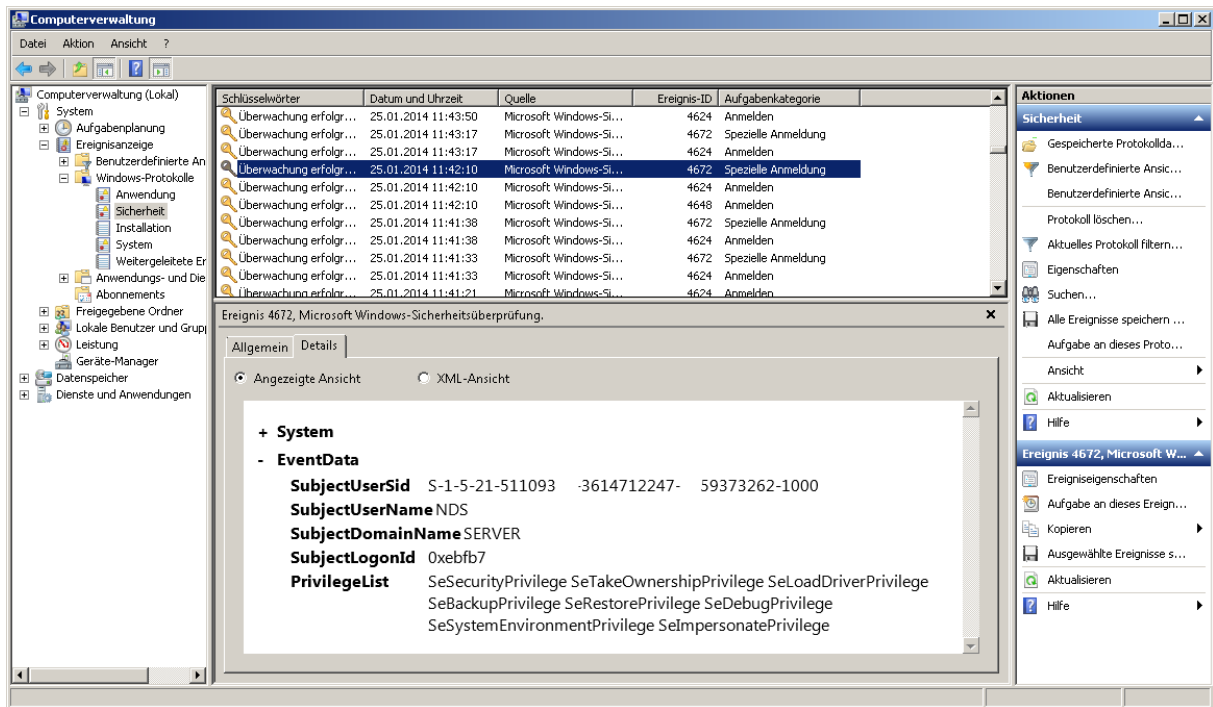
```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\NDS>whoami /user
BENUTZERINFORMATIONEN
-----
Benutzername SID
=====
server\nds S-1-5-21-511093-3614712247-59373262-1000
C:\Users\NDS>_
```

Bei Problemen mit dem System oder Anwendungen, siehe **Event-Logs**, kann die SID eine sehr elementare Information sein.

Wenn wir uns mal die Einträge in der **Sicherheit** anschauen, werden wir einen Eintrag finden, der darauf hindeutet, dass jemand die Besitzrechte eines Ordners oder einer Datei übernommen hat. Aus diesem LOG geht außerdem hervor, dass es zu jedem Benutzer auf dem System eine feste SID gibt.

Veränderungen die wir am System vornehmen, An- und Abmeldungen usw. werden protokolliert. Anhand der SID ist derjenige der sie ausgelöst hat, immer zu identifizieren.

# Windows 7 - Whoami

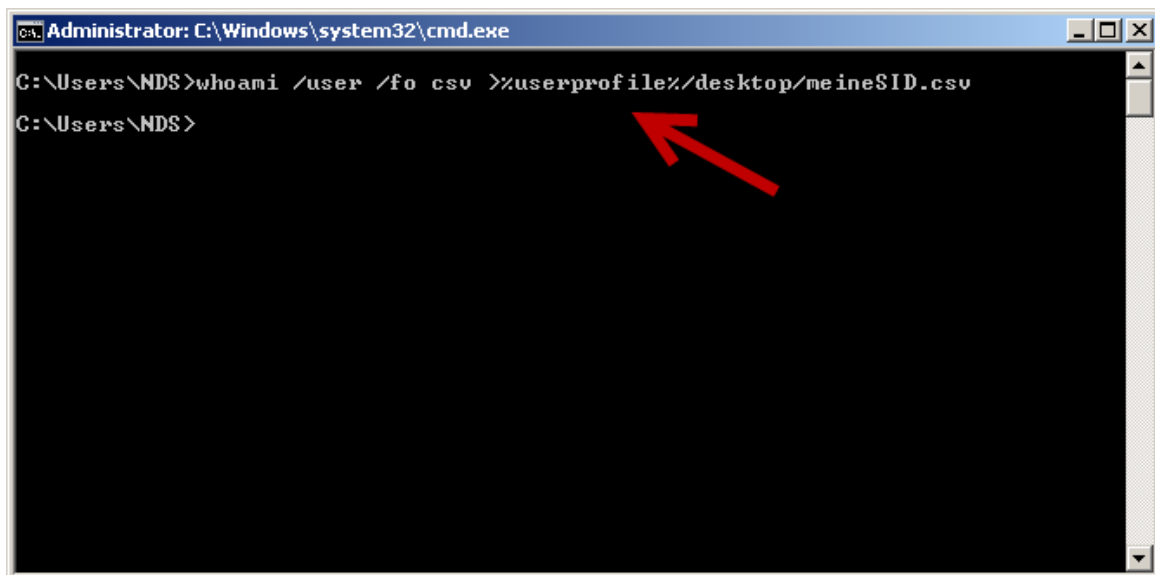


Nun gehen wir einen Schritt weiter.

Wir exportieren unsere SID in eine .csv Datei und öffnen diese mit Excel.

Über die CMD führen wir diesen Befehl aus:

**whoami /user /fo csv >%userprofile%/desktop/meineSID.csv**

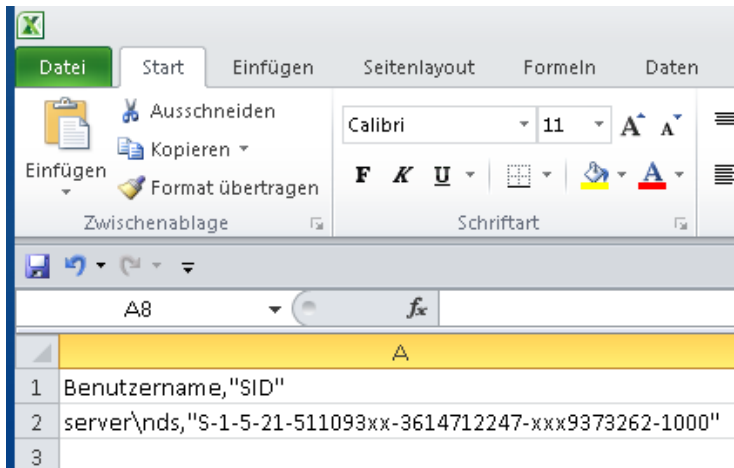


Auf dem Desktop finden wir nun die .csv Datei, meineSID.csv.



## Windows 7 - Whoami

Der Inhalt deckt sich mit dem aus der DOS-BOX.



Jetzt exportieren wir alle bekannten SIDs und zwar mit dem Befehl:

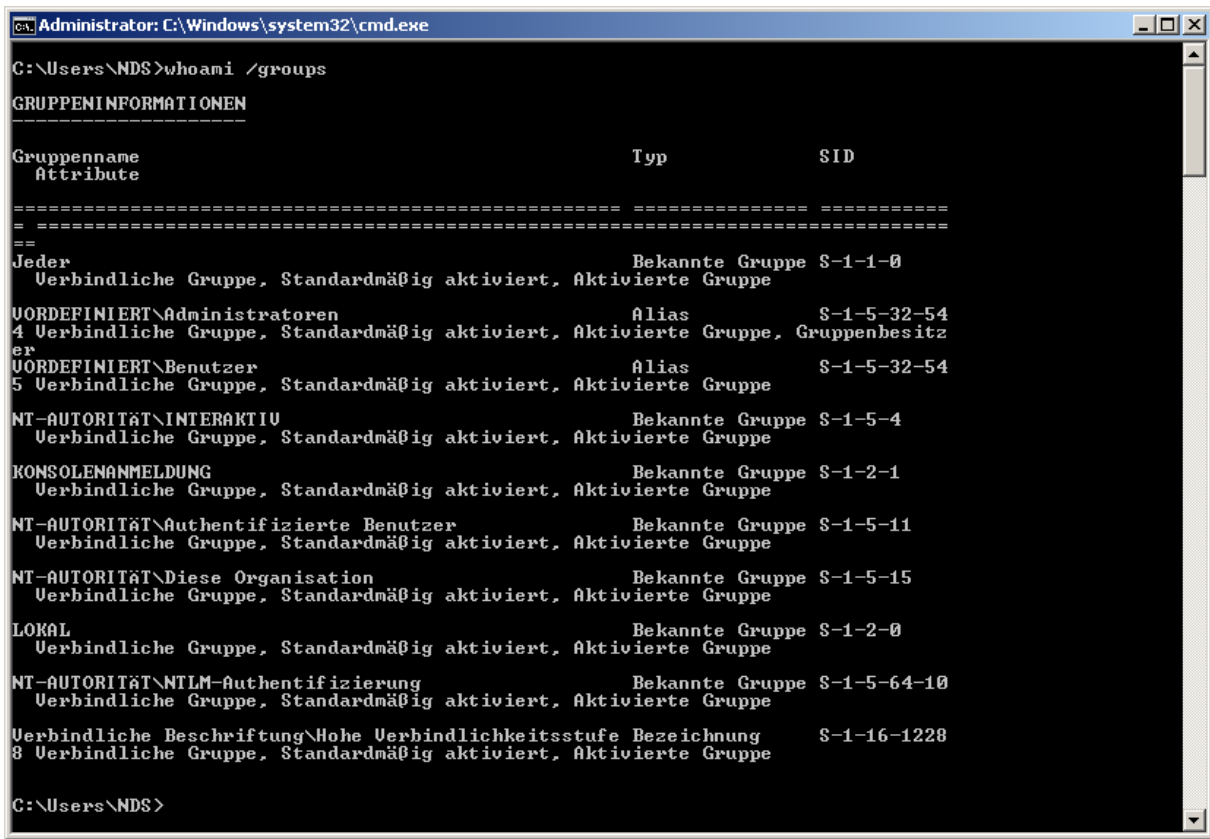
**whoami /all /fo list >%userprofile%/desktop/meineSIDs.csv**

	A	B	C	D	E	F	G	H
1								
2	BENUTZERINFORMATIONEN							
3	-----							
4								
5	Benutzername: server\\nds							
6	SID: S-1-5-21-511093xx-3614712247-xx59373262-1000							
7								
8								
9	GRUPPENINFORMATIONEN							
10	-----							
11								
12	Gruppenname: Jeder							
13	Typ: Bekannte Gruppe							
14	SID: S-1-1-0							
15	Attribute: Verbindliche Gruppe, Standardm,,áig aktiviert, Aktivierte Gruppe							
16								
17	Gruppenname: VORDEFINIERT\\Administratoren							
18	Typ: Alias							
19	SID: S-1-5-32-544							
20	Attribute: Verbindliche Gruppe, Standardm,,áig aktiviert, Aktivierte Gruppe, Gruppenbesitzer							
21								
22	Gruppenname: VORDEFINIERT\\Benutzer							
23	Typ: Alias							
24	SID: S-1-5-32-545							
25	Attribute: Verbindliche Gruppe, Standardm,,áig aktiviert, Aktivierte Gruppe							

Die Liste ist recht lang und beinhaltet darüber hinaus auch noch Informationen zu „Berechtigungsinformationen“.

## Windows 7 - Whoami

Mit dem Befehl **whoami /groups** lassen wir uns anzeigen in welchen Gruppen wir uns mit unserer aktuellen Logon-Session befinden.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\NDS>whoami /groups
GRUPPENINFORMATIONEN
-----
Gruppenname                               Typ                               SID
Attribute
=====
Jeder                                     Bekannte Gruppe                  S-1-1-0
Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
UORDEFINIERT\Administratoren             Alias                            S-1-5-32-54
4 Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe, Gruppenbesitzer
UORDEFINIERT\Benutzer                     Alias                            S-1-5-32-54
5 Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\INTERAKTIVE                 Bekannte Gruppe                  S-1-5-4
Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
KONSOLEANMELDUNG                         Bekannte Gruppe                  S-1-2-1
Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\Authentifizierte Benutzer   Bekannte Gruppe                  S-1-5-11
Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\Diese Organisation          Bekannte Gruppe                  S-1-5-15
Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
LOKAL                                     Bekannte Gruppe                  S-1-2-0
Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\NTLM-Authentifizierung       Bekannte Gruppe                  S-1-5-64-10
Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
Verbindliche Beschriftung\Hohe Verbindlichkeitsstufe Bezeichnung
8 Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe

C:\Users\NDS>
```

In einer Domäne lassen sich weitere Informationen ermitteln und anzeigen.

Jetzt möchten wir wissen welche **Berechtigungen** wir haben. Das lassen wir uns mit dem Befehl **whoami /user /priv** anzeigen. Das Ergebnis sehen wir auf der nächsten Seite.

Als Einführung in den Befehl whoami (who i am) sollte diese kleine Lektüre reichen.

## Windows 7 - Whoami

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\NDS>whoami /user /priv
BENUTZERINFORMATIONEN
-----
Benutzername SID
-----
server\nds S-1-5-21-511093-3614712247-59373262-1000

BERECHTIGUNGSMFORMATIONEN
-----
Berechtigungsnamen Beschreibung Status
-----
SeIncreaseQuotaPrivilege Anpassen von Speicherkontingenten für einen Prozess Deaktiviert
SeSecurityPrivilege Verwalten von Überwachungs- und Sicherheitsprotokollen Deaktiviert
SeTakeOwnershipPrivilege Übernehmen des Besitzes von Dateien und Objekten Deaktiviert
SeLoadDriverPrivilege Laden und Entfernen von Gerätetreibern Deaktiviert
SeSystemProfilePrivilege Erstellen eines Profils der Systemleistung Deaktiviert
SeSystemTimePrivilege ändern der Systemzeit Deaktiviert
SeProfileSingleProcessPrivilege Erstellen eines Profils für einen Einzelprozess Deaktiviert
SeIncreaseBasePriorityPrivilege Anheben der Zeitplanungspriorität Deaktiviert
SeCreatePagefilePrivilege Erstellen einer Auslagerungsdatei Deaktiviert
SeBackupPrivilege Sichern von Dateien und Verzeichnissen Deaktiviert
SeRestorePrivilege Wiederherstellen von Dateien und Verzeichnissen Deaktiviert
SeShutdownPrivilege Herunterfahren des Systems Deaktiviert
SeDebugPrivilege Debuggen von Programmen Deaktiviert
SeSystemEnvironmentPrivilege Verändern der Firmwareumgebungsvariablen Deaktiviert
SeChangeNotifyPrivilege Auslassen der durchsuchenden Überprüfung Aktiviert
SeRemoteShutdownPrivilege Erzwingen des Herunterfahrens von einem Remotesystem aus Deaktiviert
SeUndockPrivilege Entfernen des Computers von der Dockingstation Deaktiviert
SeManageVolumePrivilege Durchführen von Volumewartungsaufgaben Deaktiviert
SeImpersonatePrivilege Annehmen der Clientidentität nach Authentifizierung Aktiviert
SeCreateGlobalPrivilege Erstellen globaler Objekte Aktiviert
SeIncreaseWorkingSetPrivilege Arbeitssatz eines Prozesses vergrößern Deaktiviert
SeTimeZonePrivilege ändern der Zeitzone Deaktiviert
SeCreateSymbolicLinkPrivilege Erstellen symbolischer Verknüpfungen Deaktiviert
C:\Users\NDS>
```

Natürlich lassen sich auch diese Informationen in eine Datei speichern.

**whoami /user /priv >%userprofile%/desktop/meineSIDs.txt**