사용자 계정과 서비스 계정

- 사용자 계정
  - 사용자와 연결되어 있음
  - 사용자가 시스템 내의 파일 액세스, 이메일 전송, 애플리케이션 작업을 수행 시 사용

- 서비스 계정
  - 서비스 계정은 시스템 간 또는 애플리케이션 간 통신을 위해 생성
  - 애플리케이션 또는 서비스 자체를 나타냄
  - 애플리케이션 또는 서비스를 대신하여 작업을 인증, 승인 및 수행하는 데 사용

윈도우 부팅 과정

- 서비스 프로그램은 윈도우가 부팅된 이후에, 로그온 되지 않은 상태에서 구동
- 서비스 프로그램 구동은 Local System Account이 수행
- Local System Account 은 시스템을 제어하는데 필요한 가장 강력한 권한을 가짐

Default Account

- DSMA(기본 시스템 관리 계정)이라고도 함
- Default Account는 다중 사용자 인식 또는 사용자 중립적인 프로세스를 실행하는 데 사용
- DSMA의 SID(보안 식별자)형식 : S-1-5-21-₩<ComputerIdentifier>-503
- Default Account group SID : S-1-5-32-581

Local System Account

- Administrator 계정보다 상위 권한을 가진 System 계정
- 종류
  - NT AUTHORITY/SYSTEM : 시스템 내에서 가장 상위 권한을 가진 계정
  - NT AUTHORITY/LOCAL SERVICE
  - NT AUTHORITY/NETWORK SERVICE
- NT AUTHORITY/LOCAL SERVICE 와 NT AUTHORITY/NETWORK SERVICE은 시스템과 네트워크 자원에 사용자 수준의 권한을 부여 받아 윈도우에서 동작하는 여러가지 서비스를 구동 시킴

- **NT AUTHORITY/LOCAL SERVICE**
  - 컴퓨터 로컬에 있고 광범위한 로컬 액세스가 필요하지 않지만,
  - 인증된 네트워크 액세스가 필요하지 않은 서비스에서 사용하는 ID
  - LocalService로 실행되는 서비스는 일반 사용자로 로컬 리소스에 액세스 허용
  - LocalSystem으로 실행되는 서비스보다 권한이 훨씬 적음

- **NT AUTHORITY/NETWORK SERVICE**
  - 광범위한 로컬 액세스는 필요하지 않지만,
  - 인증된 네트워크 액세스가 필요한 서비스에서 사용되는 ID
  - NetworkService로 실행되는 서비스는 일반 사용자로 로컬 리소스에 액세스하고 컴퓨터의 ID를 사용하여 네트워크 리소스에 액세스
  - NetworkService로 실행되는 서비스는 LocalSystem으로 실행되는 서비스와 동일한 네트워크 액세스 권한을 가지지만 로컬 액세스가 크게 감소

- 시작 > 실행 > wmic > useraccount list brief

```
wmic:root\cli>useraccount list brief
AccountType  Caption                          Domain           FullName   Name               SID
512          DESKTOP-T79SQGC\Administrator    DESKTOP-T79SQGC             Administrator      S-1-5-21-2585912412-2294677559-1832327496-500
512          DESKTOP-T79SQGC\DefaultAccount   DESKTOP-T79SQGC             DefaultAccount     S-1-5-21-2585912412-2294677559-1832327496-503
512          DESKTOP-T79SQGC\Guest            DESKTOP-T79SQGC             Guest              S-1-5-21-2585912412-2294677559-1832327496-501
512          DESKTOP-T79SQGC\sora             DESKTOP-T79SQGC  Sora Kwon  sora               S-1-5-21-2585912412-2294677559-1832327496-1001
512          DESKTOP-T79SQGC\WDAGUtilityAccount DESKTOP-T79SQGC           WDAGUtilityAccount S-1-5-21-2585912412-2294677559-1832327496-504
```

* WMIC(Windows Management Instruction Console) : 윈도우 관리 명령 콘솔

  - WMIC를 이용하여 윈도우 보안 식별자를 확인 할 수 있음

잘 알려진 보안 식별자 목록

SID	설명
S-1-1-0	모든 사용자
S-1-5-14	원격 상호 로그온 접속(Remote Interactive Logon)
S-1-5-18	로컬 시스템(local system), 운영체제가 사용하는 서비스 계정
S-1-5-19	NT 권한, 로컬서비스
S-1-5-20	NT 권한, 네트워크 서비스
S-1-5-29	네트워크 서비스
S-1-5-domain-500	시스템 관리자를 위한 사용자 계정
S-1-5-domain-501	개인계정이 없는 게스트 사용자 계정, 암호를 요구하지 않고 활성화 되지 않음
S-1-5-domain-512	도메인 관리자, 소속된 사용자들이 도메인을 관리할 수 있는 전역 그룹
S-1-5-domain-513	도메인 사용자
S-1-5-domain-514	도메인 게스트, 도메인 내장 게스트 계정(한 명의 멤버만을 가지는 전역그룹)

잘 알려진 보안 식별자 목록

SID	설명
S-1-6	사이트 서버 권한(Site Server Authority)
S-1-7	인터넷 사이트 권한(Internet Site Authority)
S-1-8	교환 권한 (Exchange Authority)
S-1-9	리소스 관리자 권한(Resource Manager Authority)

\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList