BaroPAM 가이드(Windows)

목차

목차 0

1. BaroPAM 설치 1

1.1 BaroPAM 설치 전 준비사항 1

1.2 BaroPAM 설치 모듈 다운로드 및 설치 1

1.3 BaroPAM 환경 설정 4

1.4 Windows Logon 방법 7

1.5 BaroPAM 제거 및 재사용 방법 8

2. BaroPAM FAQ 10

3. About BaroPAM 13

1. BaroPAM 설치

1.1 BaroPAM 설치 전 준비사항

BaroPAM을 사용할려고 하면 사용하는 Windows 로그온 계정에 대한 암호를 반드시 설정해야 하며, Windows 로그온 계정과 암호가 맞는지 반드시 확인해야 하며, Windows에 대한 최신 Update가 되어 있는지 확인 해야 한다.

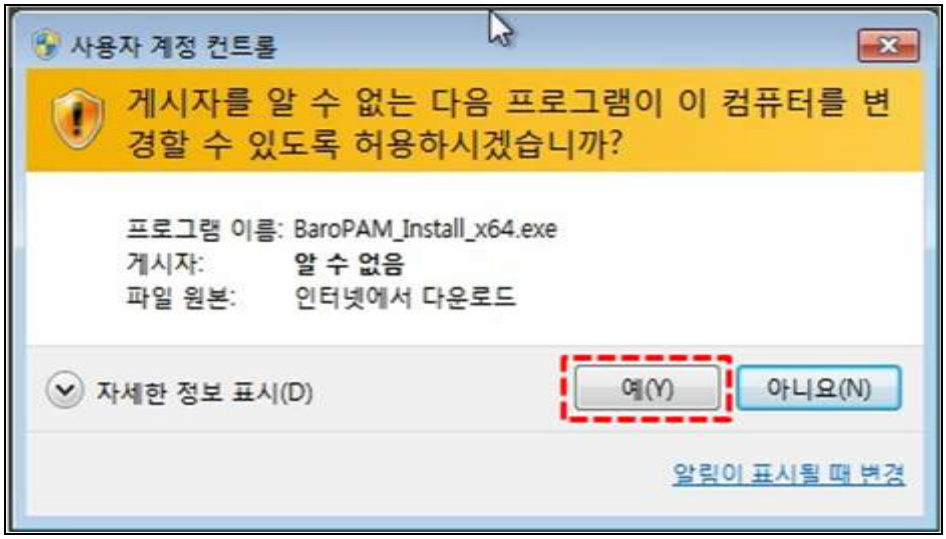
1.2 BaroPAM 설치 모듈 다운로드 및 설치

BaroPAM 설치 모듈의 다운로드할 URL은 다음과 같다.

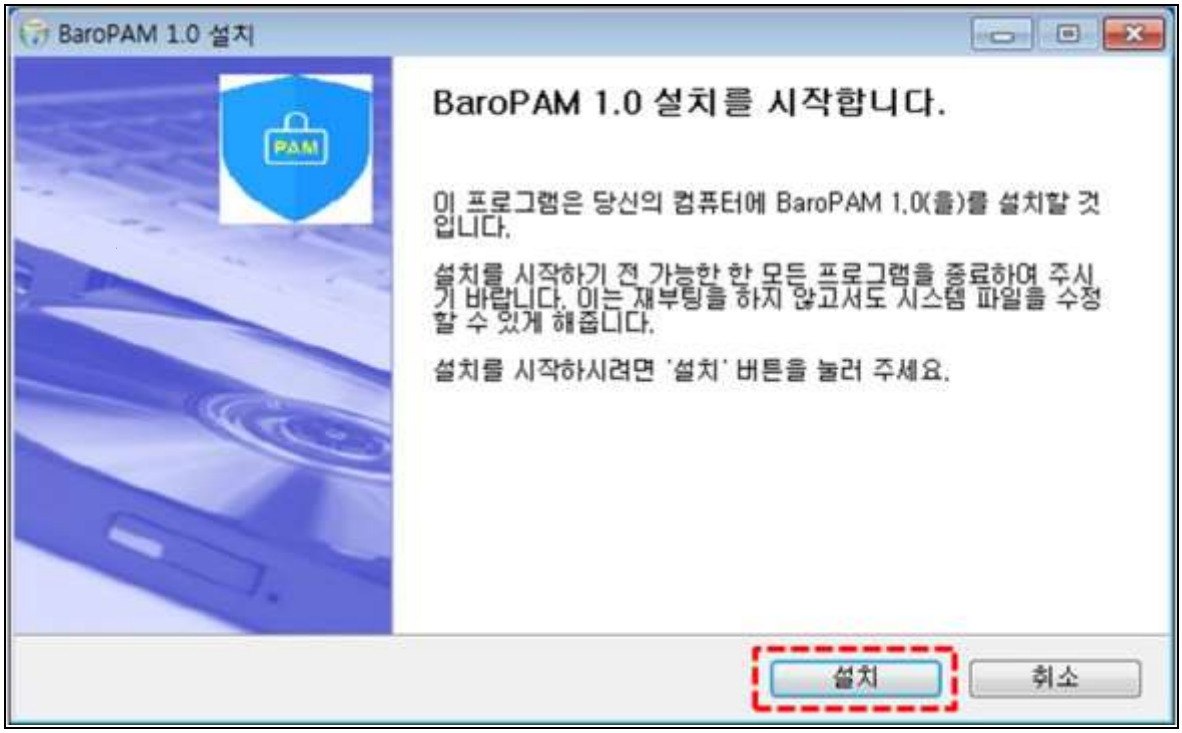
http://nuriapp.com/download/baropam_x32_v1.zip	➔ Windows 7, 32bit
http://nuriapp.com/download/baropam_x64_v1.zip	➔ Windows 7, 64bit

BaroPAM 설치는 BaroPAM 설치 모듈를 다운로드 받은 디렉토리로 이동하여 다음과 같은 순서로 BaroPAM을 설치한다.

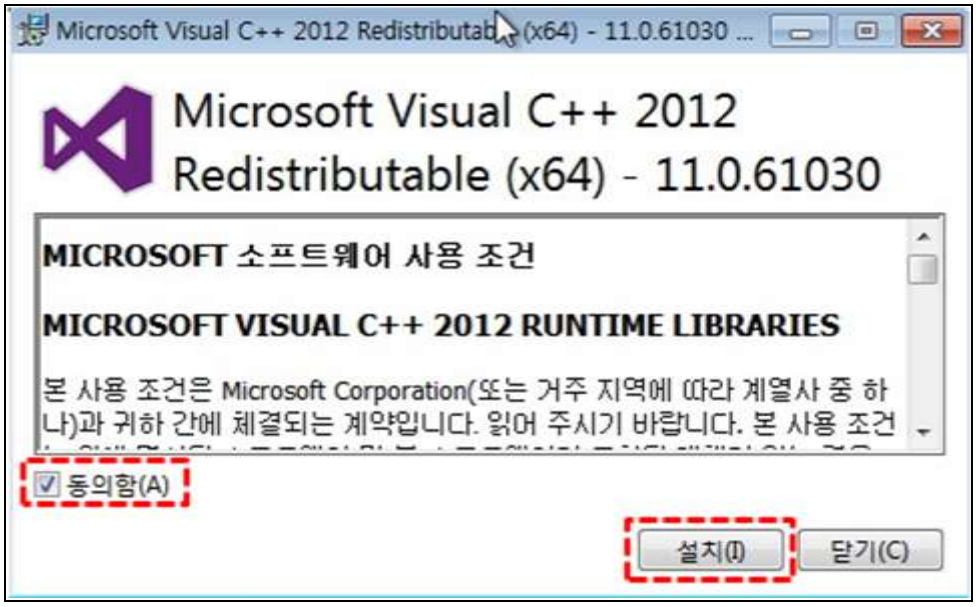
첫번째, BaroPAM 설치 파일을 클릭하면 다음과 같은 "사용자 계정 컨트롤" 화면이 나타난다.



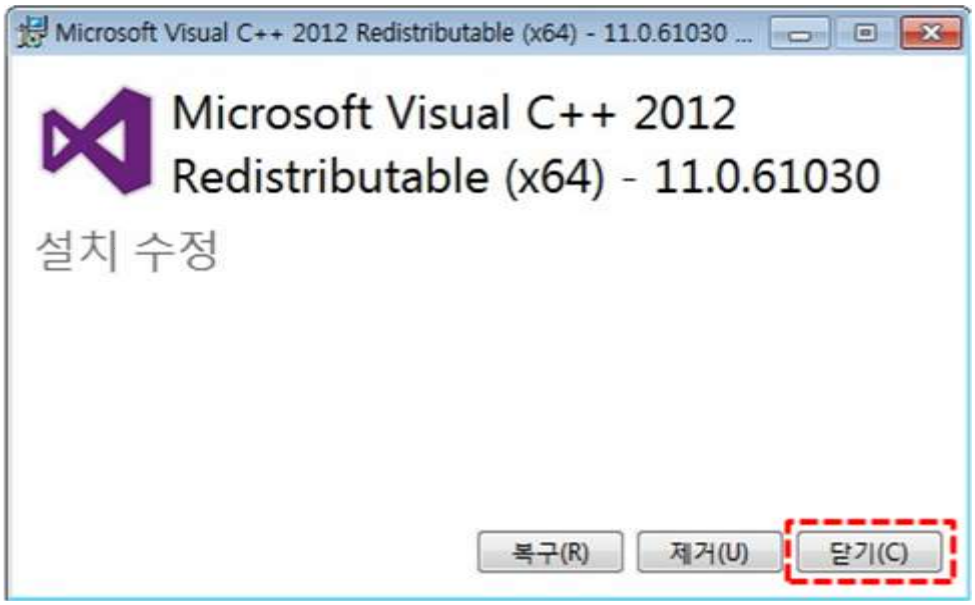
두번째, BaroPAM 설치는 반드시 관리자 계정으로 해야 되기 때문에 "**사용자 계정 컨트롤**" 화면의 내용을 확인한 후 "**예(Y)**" 버튼을 클릭해야 한다. 그러면 다음 같이 "**BaroPAM 1.0 설치**" 화면이 나타난다.



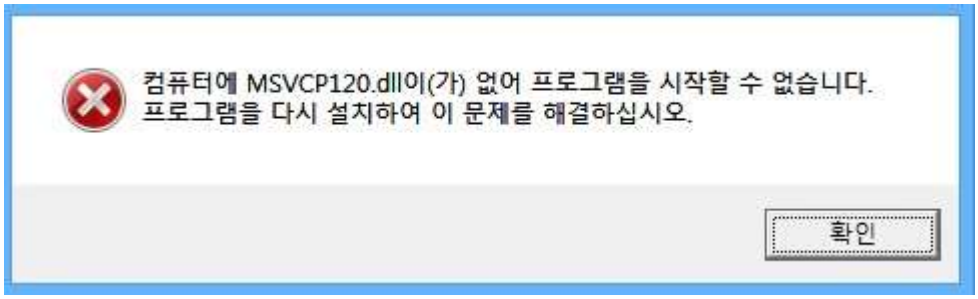
세번째, "**BaroPAM 1.0 설치**" 화면의 내용을 확인한 후 "**설치**" 버튼을 클릭하면 다음과 같이 "**Microsoft Visual C++ 2012 Redistributable**" 설치 화면이 나타난다.



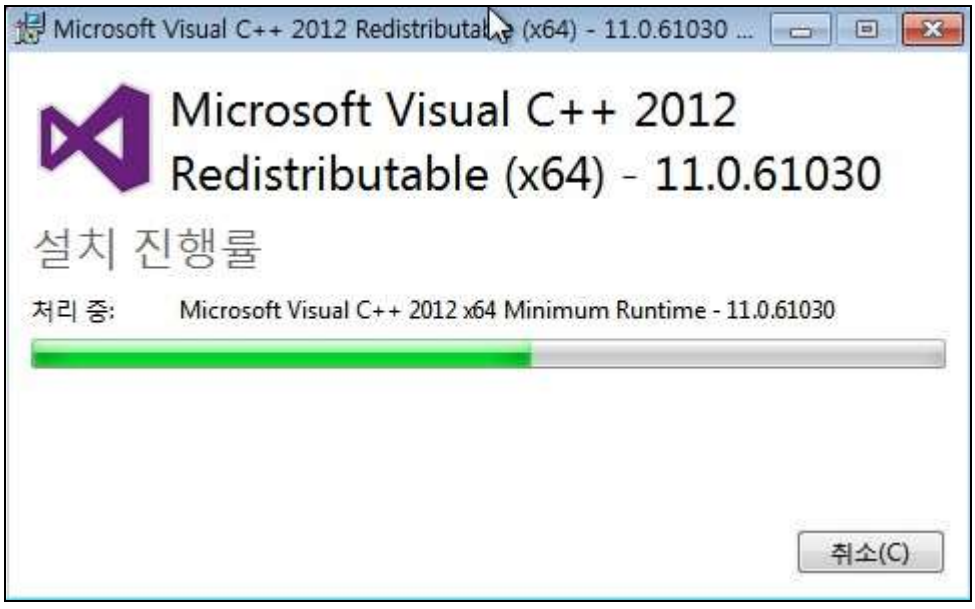
만약 이미 설치 되어 있는 경우에는 다음과 같은 "**Microsoft Visual C++ 2012 Redistributable**" 설치 수정 화면이 나타난다. 이런 경우 이미 설치되어 있기 때문에 "**닫기(C)**" 버튼을 클릭한다.



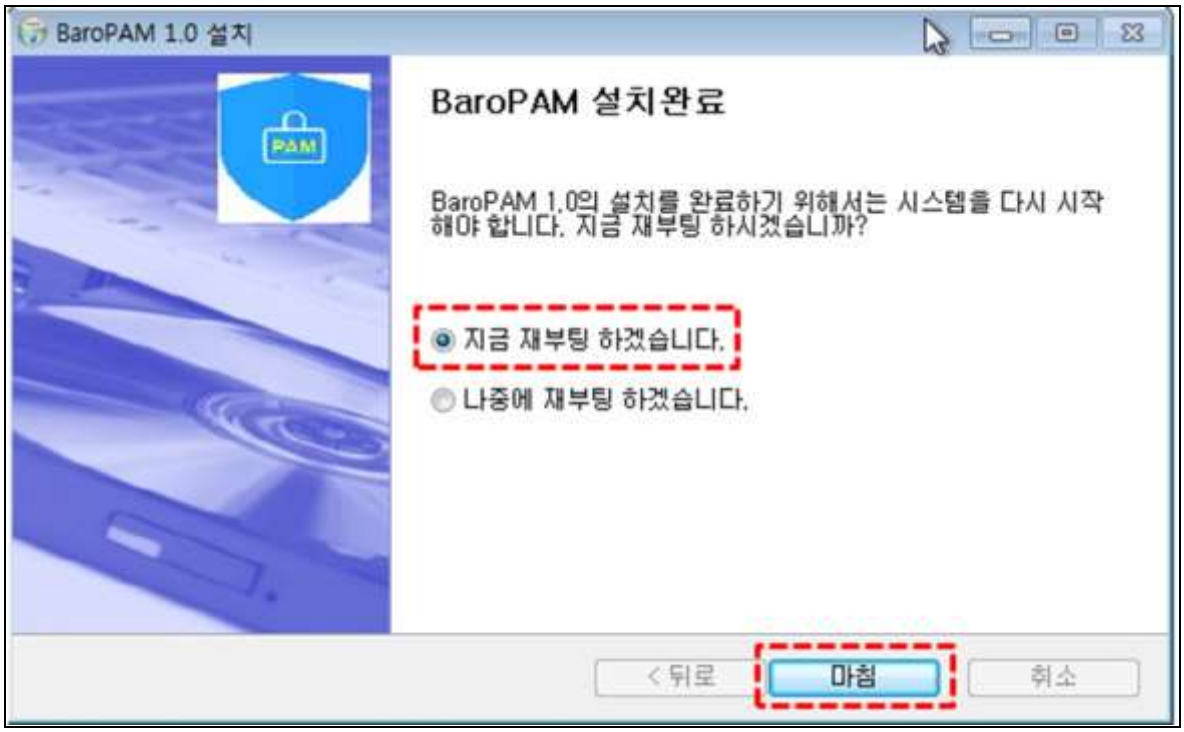
Visual Studio 2005 이후 Version으로 개발된 C++ 프로그램들은 Redistributable를 설치해야 제대로 실행되는 경우가 Windows 로그온 시 다음과 같은 오류 메시지가 발생하며 BaroPAM이 적용되지 않는다.



네번째, "**Microsoft Visual C++ 2012 Redistributable**" 설치 화면에서 "MICROSOFT 소프트웨어 사용 조건"을 확인 한 후 "**동의함(A)**"을 선택하고 "**설치(I)**" 버튼을 그러면 다음과 같이 "**설치 진행률**" 화면이 나타난다.



다섯번째, "**Microsoft Visual C++ 2012 Redistributable**"과 "**BaroPAM**" 설치가 롼료 되면 다음과 같은 "**BaroPAM 설치완료**" 화면이 나타난다.



"BaroPAM" 설치가 완료되면 "**C:₩Windows₩System32**" 디렉토리로 다음과 같은 모듈이 설치된다.

```
- 설정파일 : pam_baro_auth.ini
- 인증화면 : pam_baro_auth_7.dll, pam_baro_auth_7.exp, pam_baro_auth_7.ilk, pam_baro_auth_7.lib
- 로고파일 : baropam_logo.bmp
- 로깅파일 : pam_baro_auth.log(설정파일명 및 위치는 BARPPAM_LOG 파라미터에 설정)
- 인증키 검증모듈 : BaroKEYx.dll, BaroKEYx.lib
- 암복호 모듈 : BaroCRYPTx.dll, BaroCRYPTx.lib
- Open SSL 모듈 : libeay32MD.dll, ssleay32MD.dll
- Registry 파일 : Register.reg, Unregister.reg
```

1.3 BaroPAM 환경 설정

BaroPAM 환경 설정 파일은 "**pam_baro_auth.ini**" 파일로 "**C:₩Windows₩System32**" 디렉토리에 존재해야 한다.

만약 없는 경우에는 BaroPAM 모듈이 오작동할 수 있으므로 주의해야 한다. BaroPAM 환경 설정 파일의 정보는 다음과 같다.

```
[BaroPAM]
SECURE_KEY=Dv/6UIzIP3s5yKE/EfseZJ6z3JC+3Xqe
CYCLE_TIME=30
CORR_TIME=0
KEY_METHOD=app512
SCRATCH_CODE=62410164
LOG_SAVE=Y
```

```
BAROPAM_LOG=c:₩pam_baro_auth.log
ACL_TYPE=allow
ACL_USER=baropam,baropam-pc

[STRING]
CAPTION_BUTTON=Certification
MESSAGE_FAIL=Certification failed. Please re-enter your verification code.
MESSAGE_CTIME=Cycle time does not exist.
MESSAGE_VCODE=Please enter Verification Code.
MESSAGE_SKEY=Secure key does not exist.
```

SECURE_KEY : Windows 당 부여 받은 Secure key
CYCLE_TIME : 인증키 생성주기(초, 3~60초)
CORR_TIME : 인증키 보증오차시간(초), 인증키 생성 방식이 카드인 경우에 사용(기본값 0)
KEY_METHOD : 인증키 생성 방식(app1, app256, card384, app512: 어플, card1, card256, card384, card512: 인증카드)
SCRATCH_CODE: 응급 스크래치 코드(8자리) - 인증키 생성기를 가지고 오지 않았거나, 컴퓨터 시간 차이 등으로 인하여 컴퓨터를 접근하지 못할 때 인증키 대신 사용.
LOG_SAVE : Windows 로그온에 다핸 인증로그 저장 여부(Y or N)
BAROPAM_LOG : Windows 로그온에 대한 디렉토리를 포함한 로깅 파일명
ACL_TYPE : 2차 인증에서 허용(allow) 또는 제외(deny) 구분
ACL_USER : 2차 인증에서 허용 또는 제외할 username을 콤마(Comma)로 구분

Windows의 로그온 시 로깅되는 인증로그의 사항과 형식은 다음과 같다.

1) 로그온 성공

① 응급 스크래치 코드 사용
2018.10.14 11:46:02-0537(UTC) : BAROPAM-PC : emergency scratch code : session opened for user root by (ip=1.234.83.169)

② 일회용 인증키 사용
2018.10.14 11:46:02-0537(UTC) : BAROPAM-PC : authentification key : session opened for user root by (ip=1.234.83.169)

2) 로그온 실패

① 검증 실패
2018.10.14 11:46:02-0537(UTC) : BAROPAM-PC : authentification key : User root authentication failed (ip = 1.234.83.169)

② 인증키 생성주기가 없음
2018.10.14 11:46:02-0537(UTC) : BAROPAM-PC : authentification key : There is no cycle time for user root (ip = 1.234.83.169)

③ 인증키를 입력하지 않음
2018.10.14 11:46:02-0537(UTC) : BAROPAM-PC : authentification key : There is no verification code for user root (ip = 1.234.83.169)

④ 인증키가 없음
2018.10.14 11:46:02-0537(UTC) : BAROPAM-PC : authentification key : There is no secure key for user root (ip = 1.234.83.169)

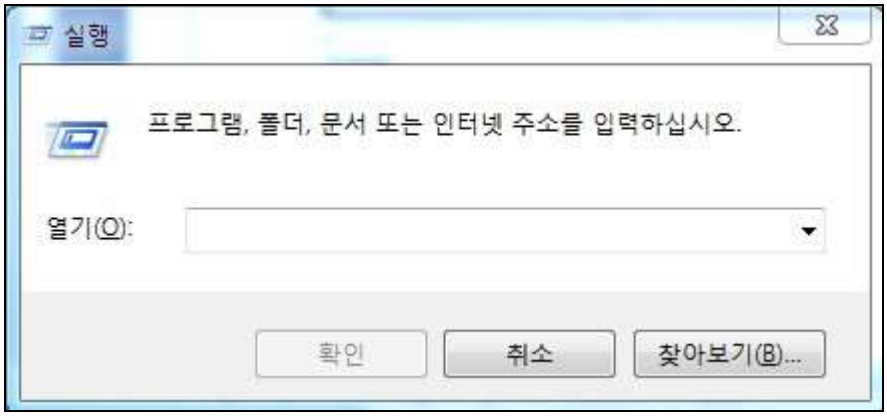
Windows 시간이 현재 시간과 다를 경우 인증키와 매칭이 되지 않아 일회용 인증키가 맞질 않으므로 시간을 같게 시간 동기화 해야 한다.

최근에는 서버/네트워크 장비에 대한 시간 동기화(타임서버 시간 동기화)하는 방법으로 NTP(Network Time Protocol)을 이용하여 관리자 계정에서 시스템의 시각을 현재 시각으로 설정할 수 있다.

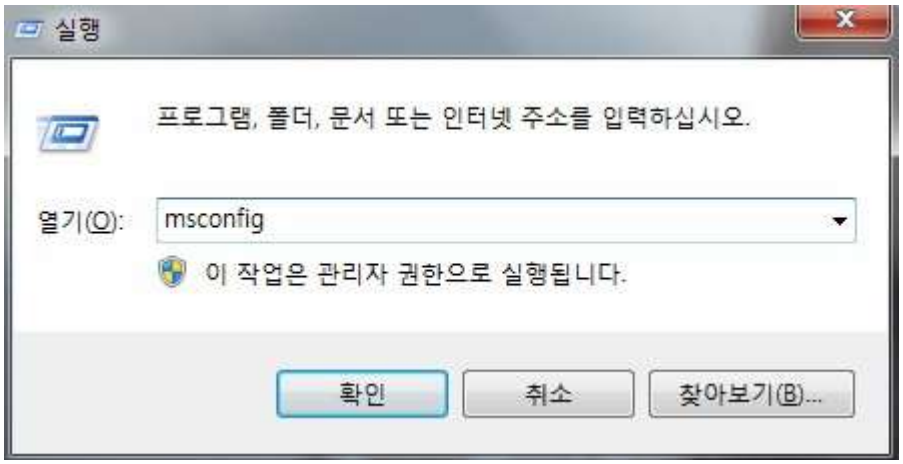
만약 Windows 로그온이 안되는 경우에는 다음과 같이 안전모드로 부팅한 후 "**C:₩Windows₩System32**" 디렉토리로 이동한 후 "**Unregister.reg**" 파일을 클릭하면 Windows registry에 추가된 BaroPAM 정보를 해제할 수 있다.

안전 모드는 운영 체제 진단을 위한 모드로 시스템을 최소한의 파일과 드라이버만 사용하는 등 기능적인 제약이 많다. 하지만 이 덕에 오히려 문제 해결에 도움을 줄 수 있다.

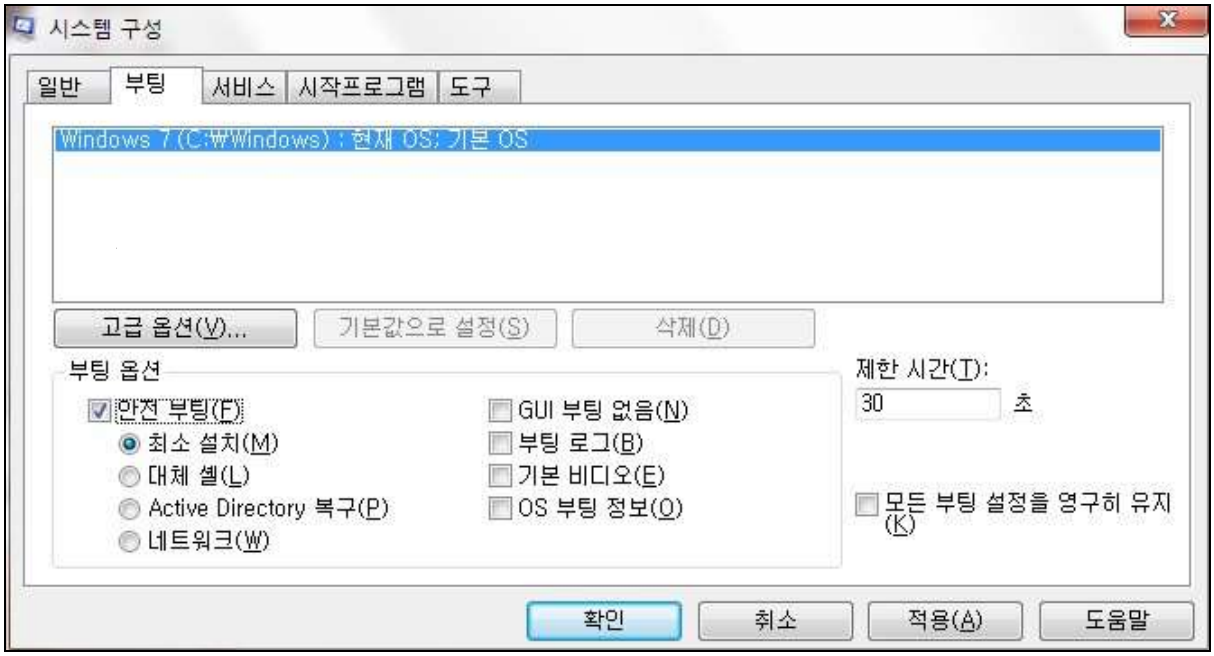
첫번째, 시작-실행을 누르든가 아니면 "윈도우 키+R"를 눌러 실행 창을 실행한다.



두번째, 열기 항목에 다음과 같이 "msconfig" 입력한 뒤 "확인" 버튼을 클릭한다.



세번째, "부팅" 탭을 선택한 후 "부팅 옵션"에서 "안정 부팅(R)"을 다음과 같이 선택한다.



기타 옵션은 바꿀 필요가 없다. 이제 재시작을 하면 안전 모드로 부팅된다. 하지만 안전 모드에서 사용이 끝난 후 다시 이 옵션을 선택 해제해야 한다.

1.4 Windows Logon 방법

Windows를 전원을 켜면 다음과 같은 BaroPAM의 인증키와 Windows의 Password를 입력하는 BaroPAM의 로그인 화면이 나타난다.

스마트 폰에서 인증키를 생성한 후 "**Verification code**"에 생성한 인증키와 Windows의 "**Password**"를 입력한 후 "**->**" 버튼을 클릭하면 BaroPAM 모듈에 인증을 요청하여 검증이 성공하면 Windows OS의 로그인 인증 정책이 작동된다.

Windows에서는 입력한 인증키를 BaroPAM 검증모듈에서 인증에 실패하면 다음과 같은 "**Error**" 메시지 박스가 나타나며 BaroPAM의 로그인 화면에 머무른다.

1.5 BaroPAM 제거 및 재사용 방법

BaroPAM이 설치된 상태에서 BaroPAM 모듈을 사용하지 않을 경우 Windows registry에 추가된 정보를 해제하기 위하여 "**C:₩Windows₩System32₩Unregister.reg**" 파일을 클릭한다. "**Unregister.reg**" 파일의 정보는 다음과 같다.

```
Windows Registry Editor Version 5.00

[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider
Filters\{75A22DF0-B81D-46ed-B119-CD30507BD615}]

[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{75A22DF0-B81D-46ed-B119-CD30507BD615}]
```

BaroPAM이 설치된 상태에서 BaroPAM 모듈을 재사용하는 경우 Windows registry에 추가하기 위하여 "**C:\Windows\System32\Register.reg**" 파일을 클릭한다. "**Register.reg**" 파일의 정보는 다음과 같다.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential   Provider
Filters\{75A22DF0-B81D-46ed-B119-CD30507BD615}]
@="baroPAMLogon"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{75A22DF0-B81D-46ed-B119-CD30507BD615}]
@="baroPAMLogon"

[HKEY_CLASSES_ROOT\CLSID\{75A22DF0-B81D-46ed-B119-CD30507BD615}]
@="baroPAMLogon"

[HKEY_CLASSES_ROOT\CLSID\{75A22DF0-B81D-46ed-B119-CD30507BD615}\InprocServer32]
@="pam_baro_auth_7.dll"
"ThreadingModel"="Apartment"
```

2. BaroPAM FAQ

현상: Windows용 BaroPAM 설치 후 로그온 시 로그온 화면이 나타나지 않고 오작동되는 현상 발생.
원인: "컴퓨터 이름" 또는 "PC의 이름"은 한글이 포함되어 있어서 발생.
조치: "탐색기 -> 내 PC -> 마우스 오른쪽 버튼 클릭 -> 속성"을 클릭하여 "컴퓨터 이름" 또는 "PC의 이름 "은 한글이 포함되어 있는지 확인한 후 반드시 "영문자, 하이픈, 숫자를 조합해서 사용"해야 한다.

현상 : 일회용 인증키가 맞지 않아서 로그인을 하지 못하는 경우
원인 : BaroPAM은 시간 동기화 방식으로 폰과 Windows나 Server의 시간이 동일해야 함,
조치 : 폰과 Windows나 Server의 시간이 맞는지 확인.

현상 : 안드로이드 폰 또는 아이폰의 날짜와 시간이 현재 시간과 차이가 발생하여 "일회용 인증키"가 맞지 않은 경우
원인 : 안드로이드 폰 또는 아이폰의 날짜와 시간을 네트워크에서 제공하는 시간을 사용하지 않아서 발생.
조치 : 안드로이드 폰인 경우는 폰의 "설정" -> "일반" -> "날짜 및 시간" -> "날짜 및 자동 설정"과 "시간대 자동 설정" -> "허용"
아이폰인 경우는 폰의 "설정" -> "날짜 및 시간" -> "자동으로 설정" -> "허용"

현상 : 로그온 스크립트 프로세스가 완료되기 위한 30초 지연 발생.
특정 마스터 이미지를 통해서 Windows OS를 배포하고 나서 로그온 하면 로그온 속도가 오래 걸리는 경우가 지속해서 발생.
원인 : Windows OS를 실행하는 컴퓨터에서 "로그온 스크립트를 동기적으로 실행" 그룹 정책을 사용하도록 설정되어 있어서 로그온을 시도할 때 시작 화면이 30초 동안 표시되며, 그런 다음 로그온 스크립트 프로세스가 완료되기 전에 로그온 스크립트가 사용자와 작동하기 때문이다.
조치 : 이 문제를 해결하려면 Timeout 간격을 30초 미만으로 변경하면 로그온 속도가 개선됨.
1. 시작 -> 실행 -> regedit.msc 레지스트리 편집기 실행
2. 다음 경로로 이동
HKEY_LOCAL_MACHINEWSOFTWAREWMicrosoftWWindowsWCurrentVersionWPoliciesWSystem
3. 다음 값 생성 또는 수정
Name : DelayedDesktopSwitchTimeout
Type : REG_DWORD
Value : 5
4. 시스템 재시작 후 로그온 속도 개선 확인.

현상 : Windows 프로그램을 삭제한 후에도 시스템 재시작시 자동으로 재설치되는 사례 발생.
원인 : PC 자동 백업 등과 같은 관리 프로그램의 해서 Windows 재기동 시 마지막 백업 받은 시점의 이미지를 로드하기 때문.
사용자가 인터넷 상에서 특정 파일을 다운로드하여 실행시 또는 프로그램 설치 후 업데이트 방식을 통해 사용자 동의를 통해 설치가 되는 것으로 추정.
실제로는 이런 설치 과정에서 사용자가 제대로 확인할 수 없도록 눈속임 또는 실수를 유발하여 설치가 이루어짐.
시작 프로그램 폴더에 등록할 경우에는 파일을 제거하지 않는 한 반복적으로 시스템 시작시마다 해당 파일을 실행함.
조치 : 시작 프로그램 폴더(C:WDocuments and SettingsW(사용자 계정)W시작 메뉴W프로그램W시작프로그램)에 등록된 파일을 찾아서 제거.

현상 : Failed to open file "Filename"[error message]"
원인 : 환경설정 파일인 Filename을 Open할 수 없는 경우에 발생.
조치 : error message를 확인한 후 환경설정 파일이 존재하는지 확인 후 BaroPAM Setup 화면에서 재설정.

현상 : Invalid RATE_LIMIT option. Check pam_baro_auth.ini
원인 : 환경설정 파일인 pam_baro_auth.ini 파일의 내용 중 RATE_LIMIT 설정값이 잘못 설정되어 있는 경우 발생.

조치 : 제한 횟수(1 < RATE_LIMIT < 100), 제한 시간(1 < interval < 3600)의 설정 값을 확인.
BaroPAM Setup 화면에서 확인 후 재설정.

현상 : Invalid list of timestamps in RATE_LIMIT. Check pam_baro_auth.ini
원인 : 환경설정 파일인 pam_baro_auth.ini 파일의 내용 중 RATE_LIMIT 옵션에 Update된 timestamps가 잘 못된 경우 발생.
조치 : 환경설정 파일인 pam_baro_auth.ini 파일의 RATE_LIMIT 옵션에 Update된 timestamps를 확인.

현상 : Try to update RATE_LIMIT line.
원인 : 정상적으로 로그인 한 경우 출력되는 메시지.
조치 : No action

현상 : Too many concurrent login attempts. Please try again.
원인 : 환경설정 파일인 pam_baro_auth.ini 파일의 DISALLOW_REUSE 옵션(일회용 인증키 생성 주기 내에는 하나의 로그인만 가능)이 설정된 경우 로그인 성공 후 일회용 인증키 생성 주기 내에 로그인을 재 시도한 경우 발생.
조치 : 일회용 인증키 생성 주기 후에 로그인 재 시도.

현상 : Can't find ACL_TYPE[error message]
원인 : 환경설정 파일인 pam_baro_auth.ini 파일의 ACL_TYPE 옵션이나 설정값이 없는 경우에 발생.
조치 : 환경설정 파일인 pam_baro_auth.ini 파일의 ACL_TYPE 옵션이나 설정값 확인.
BaroPAM Setup 화면에서 확인 후 재설정.

현상 : Can't find ACL_FILE[error message]
원인 : ACL 파일인 pam_baro_acl.ini 파일의 ACL_FILE 옵션이나 설정값이 없는 경우에 발생.
조치 : ACL 파일인 pam_baro_acl.ini 파일의 ACL_FILE 옵션이나 설정값 확인.
BaroPAM Setup 화면에서 확인 후 재설정.

현상 : Invalid WINDOW_SIZE option in pam_baro_auth.ini
원인 : 환경설정 파일인 pam_baro_auth.ini 파일의 내용 중 WINDOW_SIZE 설정값(현재 시간을 기준으로 보정시간)이 잘못 설정되어 있는 경우 발생.
조치 : 현재 시간을 기준으로 일회용 인증키 보정시간(1 < WINDOW_SIZE < 100)의 설정 값을 확인.

현상 : Trying to reuse a previously used time-based code.
Retry again in 30 seconds.
Warning! This might mean, you are currently subject to a man-in-the-middle attack.
원인 : 환경설정 파일인 pam_baro_auth.ini 파일의 DISALLOW_REUSE 옵션은 중간자 공격(man-in-the-middle)을 대비한 옵션.
중간자 공격(man-in-the-middle)은 권한이 없는 개체가 두 통신 시스템 사이에서 스스로를 배치하고 현재 진행 중인 정보의 전달을 가로채면서 발생. 간단히 말해서, 현대판 도청 시스템이라고 할 수 있는 것
조치 : No action

현상 : Failed to allocate memory when updating pam_baro_auth.ini
원인 : 환경설정 파일인 pam_baro_auth.ini를 업데이트 할 때 메모리 할당에 실패한 경우 발생.
조치 : Technical support

현상 : Can't find HOSTNAME[error message]
원인 : 환경설정 파일인 pam_baro_auth.ini 파일의 HOSTNAME 옵션이나 설정값이 없는 경우에 발생.
조치 : 환경설정 파일인 pam_baro_auth.ini 파일의 HOSTNAME 옵션이나 설정값 확인.
BaroPAM Setup 화면에서 확인 후 재설정.

현상 : Can't find SECURE_KEY[error message]

원인 : 환경설정 파일인 pam_baro_auth.ini 파일의 SECURE_KEY 옵션이나 설정값이 없는 경우에 발생.
조치 : 환경설정 파일인 pam_baro_auth.ini 파일의 SECURE_KEY 옵션이나 설정값 확인.
BaroPAM Setup 화면에서 확인 후 재설정.

현상 : Can't link DB [error message]
원인 : DB 파일인 pam_baro_db.ini 파일의 DB link 옵션이나 설정값이 없는 경우에 발생.
조치 : DB 파일인 pam_baro_db.ini 파일의 DB link 옵션이나 설정값 확인.
BaroPAM Setup 화면에서 확인 후 재설정.

현상 : Invalid verification code
원인 : 일회용 인증키 검증에 실패한 경우 발생.
조치 : 로그인 재 시도.

3. About BaroPAM

Version 1.0 - Official Release - 2016.12.1

http://www.nurit.co.kr

제 조 사 : 주식회사 누리아이티
등록번호 : 258-87-00901
대표이사 : 이종일
대표전화 : 02-2665-0119(영업문의/기술지원)
이 메 일 : mc529@nurit.co.kr
주 소 : 서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)