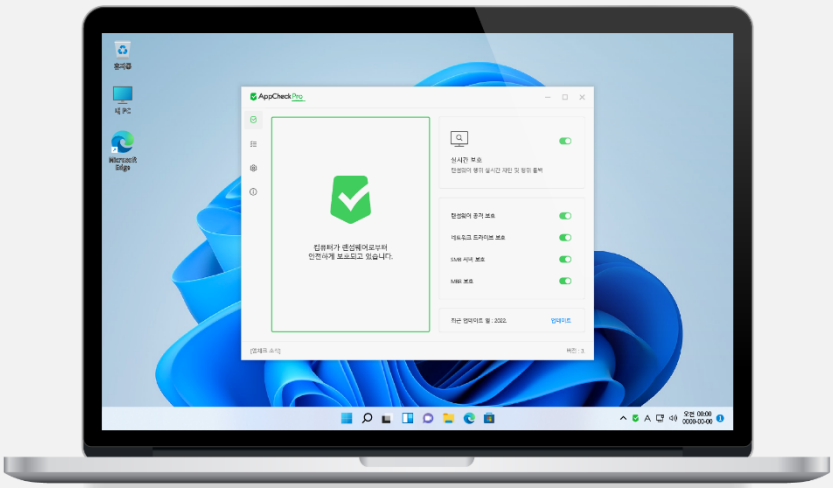
AppCheck Pro

안티랜섬웨어 도움말



NEVER MIND THE SECURITY

AppCheck can be used with other various vaccines without conflict thanks to its minimum usage capacity and use of system resources. It boasts greater safety by blocking even ransomware infections that come through networks.

CHECKMAL

목차

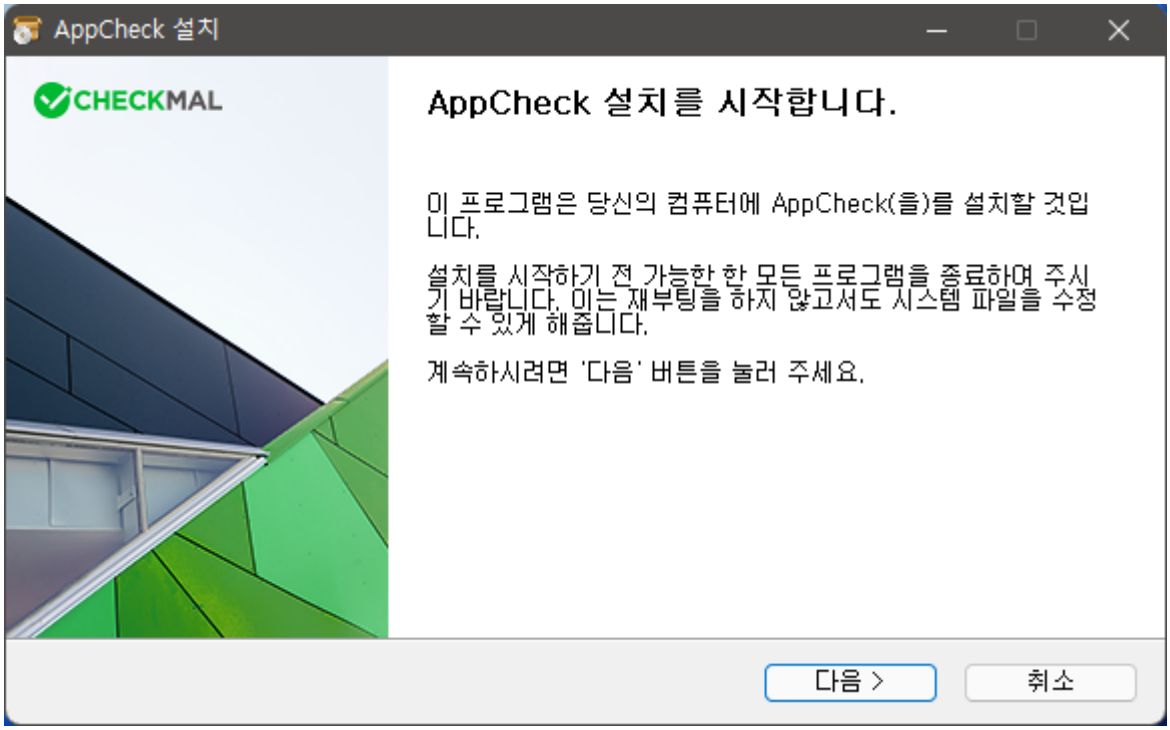
1. AppCheck 매뉴얼 이력 관리

문서 버전	작성일	제품 버전	내용
1.0	2023년 3월 1일	3.1.27.4	버전 업데이트에 따른 내용 수정
1.1	2023년 6월 4일	3.1.31.2	버전 업데이트에 따른 내용 수정
1.2	2023년 8월 15일	3.1.33.7	버전 업데이트에 따른 내용 수정
1.3	2024년 3월 28일	3.1.36.2	버전 업데이트에 따른 내용 수정

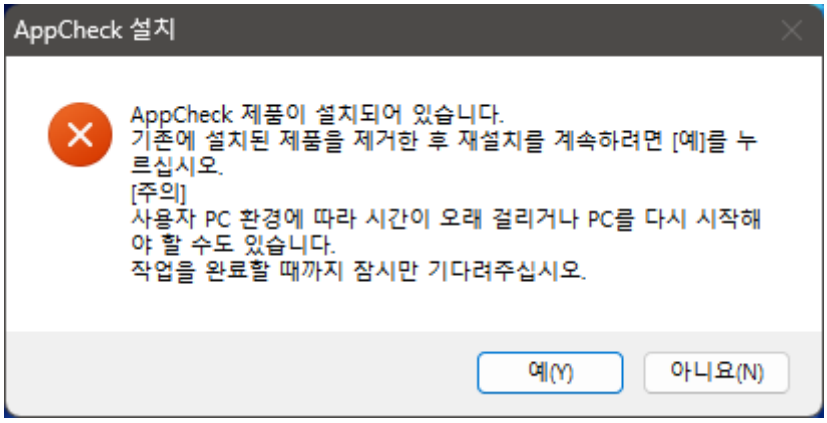
2. AppCheck : 설치하기

AppCheck (이하 AppCheck) 제품은 Windows 7 SP1 (Microsoft SHA-2 패치 사전 설치 필요 : KB4474419), Windows 8, Windows 8.1, Windows 10, Windows 11 운영 체제(32/64 Bit) 환경에서 설치하여 사용할 수 있으며, 한국어 / 영어 / 일본어 운영 체제에 따라 자동으로 설치 언어가 변경된다.

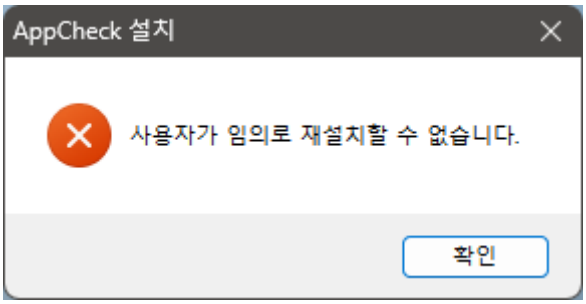
(1) AppCheck를 설치하기 전 실행 중인 모든 프로그램을 종료한 후 설치를 진행한다.



만약 AppCheck 제품이 이미 설치되어 있다면 "AppCheck 제품이 설치되어 있습니다. 기존에 설치된 제품을 제거한 후 재설치를 계속하려면 [예]를 누르십시오. [주의] 사용자 PC 환경에 따라 시간이 오래 걸리거나 PC를 다시 시작해야 할 수도 있습니다. 작업을 완료할 때까지 잠시만 기다려 주십시오." 안내 메시지 창이 생성된다.

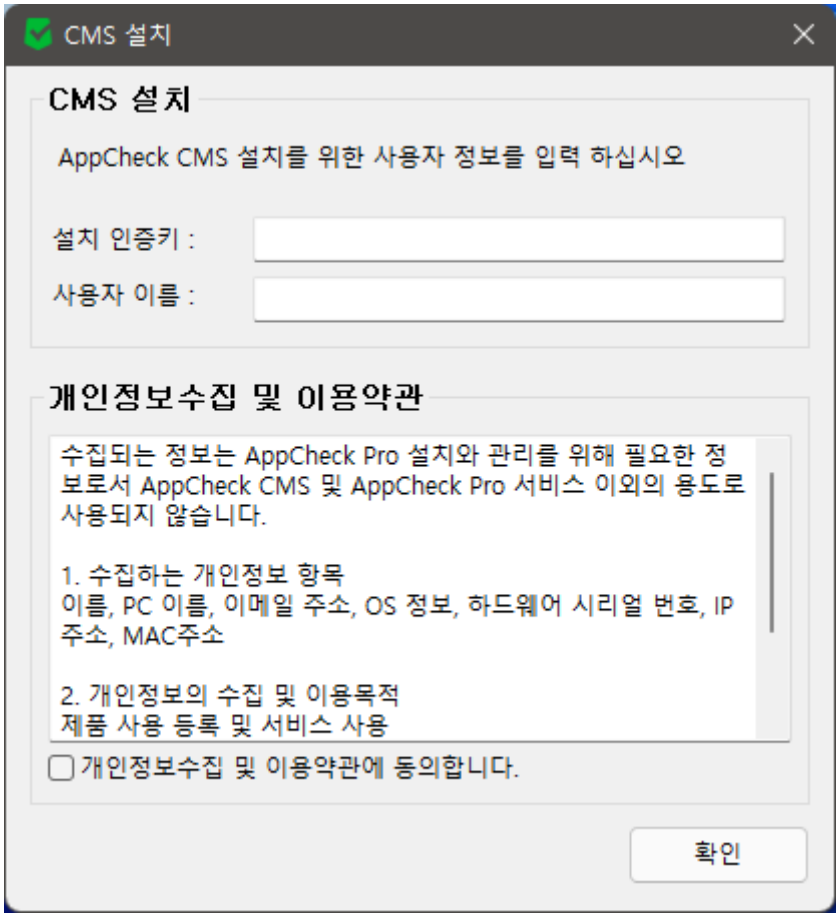


- **예(Y) :** "사용자가 임의로 재설치할 수 없습니다." 안내창 생성을 통한 재설치 중단
- **아니요(N) :** 추가적인 안내창 생성없이 재설치 중단



위와 같이 AppCheck 제품이 설치되어 있는 환경에서 AppCheck 설치 파일을 이용한 재설치는 기본적으로 허용하지 않는다.

CMS Cloud 또는 CMS Business 중앙 관리 사이트의 배포 관리에서 제공하는 AppCheck 설치 파일을 이용하여 AppCheck 설치 시에는 반드시 CMS 서버와 통신이 이루어져야 한다.

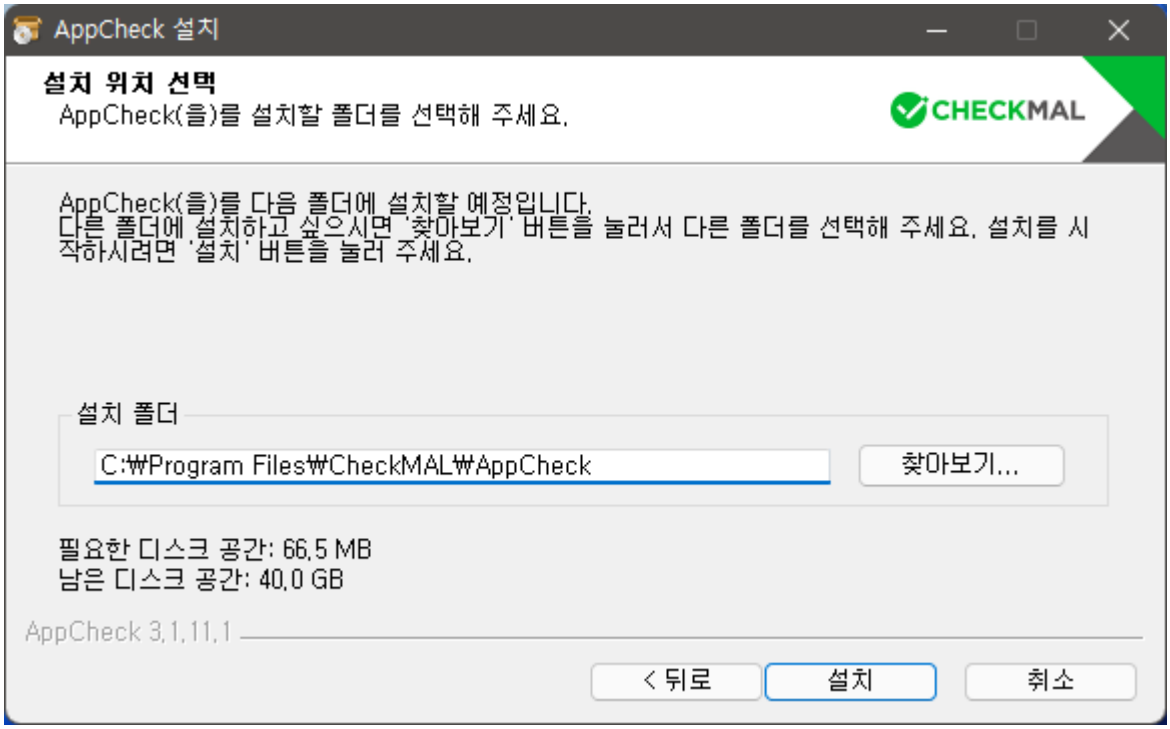


- **설치 인증키 :** 기본적으로 자동 입력되어 있으며, CMS 배포 관리에서 제공하는 설치 인증키와 동일하다.
- **사용자 이름 :** 기본값은 Windows 사용자 계정명으로 표시되며, 회사 정책에 따라 식별 가능한 사용자 이름으로 수정 가능하다.

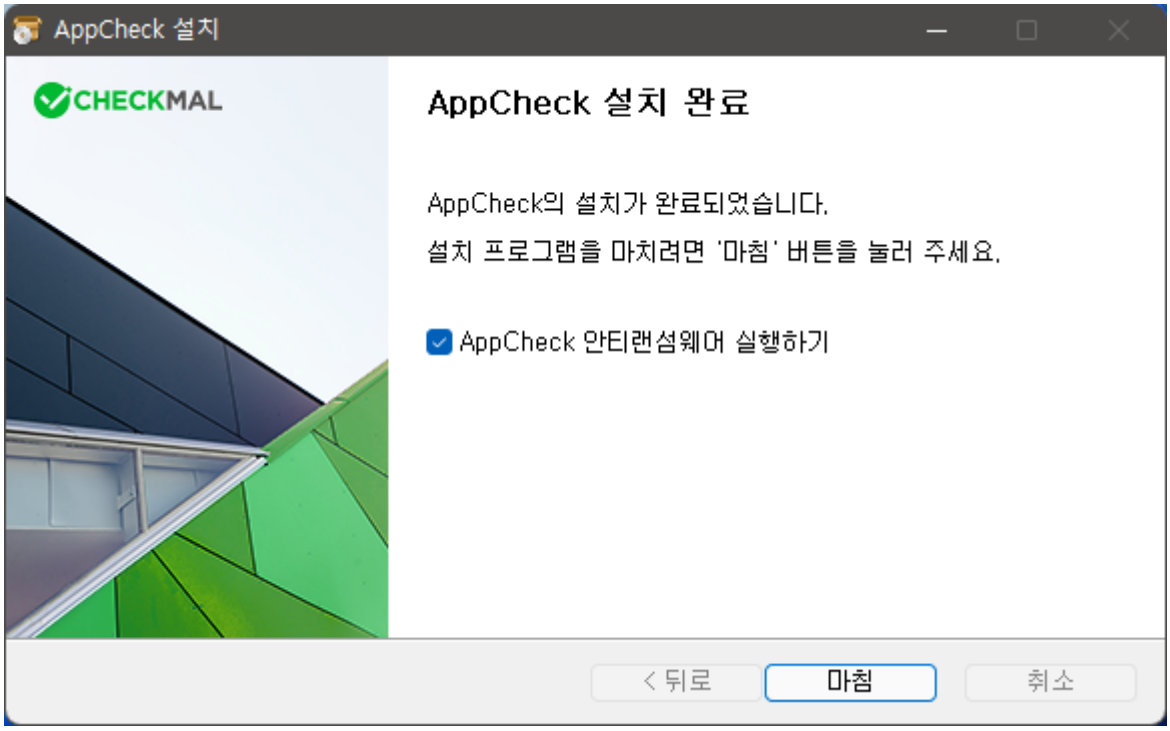
생성된 CMS 설치창에 정보 입력 후 "개인정보수집 및 이용약관에 동의합니다." 박스에 체크 후 "확인" 버튼을 클릭한다. 단, AppCheck 설치 파일명을 임의로 변경할 경우 자동 등록된 "설치 인증키"가 표시되지 않으므로 직접 입력해야 한다.

(2) ㈜체크멀 소프트웨어 사용권 계약서 내용에 확인 후 "동의함" 버튼을 클릭한다.

(3) AppCheck는 "C:₩Program Files₩CheckMAL₩AppCheck" 기본 설치 폴더(32/64bit 공통)에 프로그램을 설치하며, 다른 폴더에 설치를 원한다면 "찾아보기..." 버튼을 클릭하여 폴더를 변경하여 설치할 수 있지만 이미 AppCheck가 설치된 경우에는 기존 설치 폴더에서 변경할 수 없다.

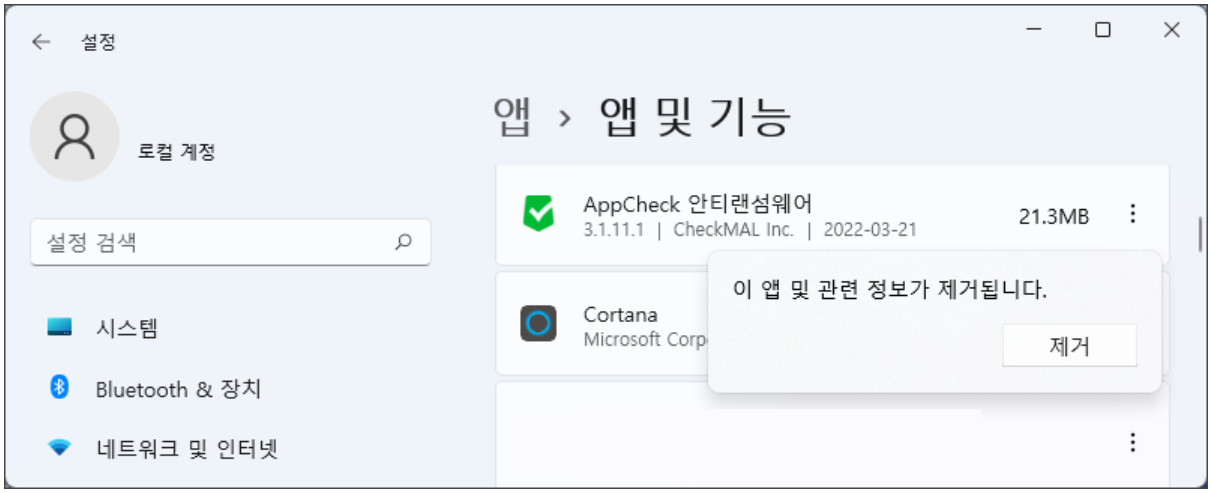


(4) AppCheck 설치가 완료된 후 "마침" 버튼을 클릭하면 AppCheck 안티랜섬웨어 프로그램이 자동 실행된다.

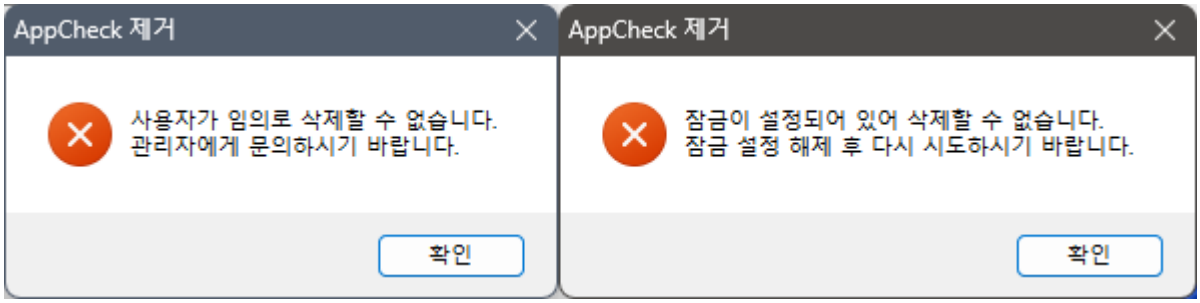


3. AppCheck : 제거하기

(1) AppCheck 제거는 "제어판 - 프로그램 – 프로그램 및 기능 – 프로그램 제거" 또는 "설정 – 앱 – 설치된 앱"에 등록된 "AppCheck 안티랜섬웨어" 프로그램을 찾아 제거 버튼을 클릭한다.



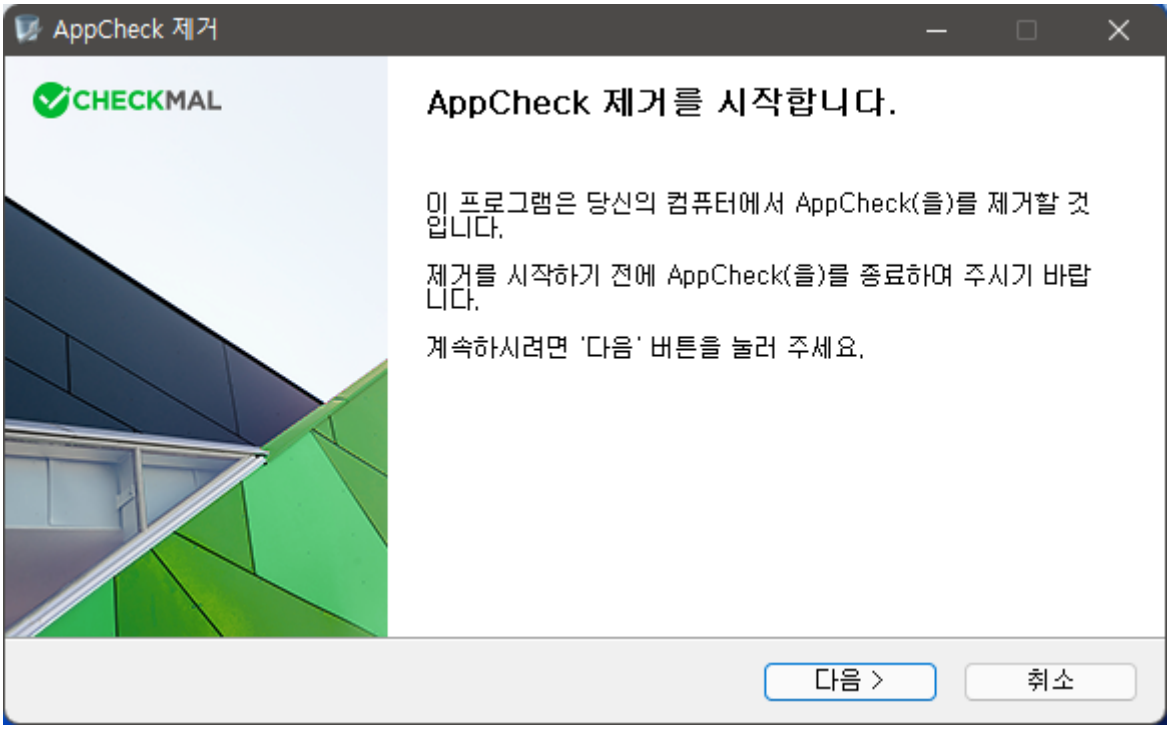
만약 AppCheck 옵션 또는 CMS 정책을 통해 AppCheck 제거를 허용하지 않을 경우 다음과 같은 메시지 창이 생성되어 AppCheck 프로그램을 삭제할 수 없다.



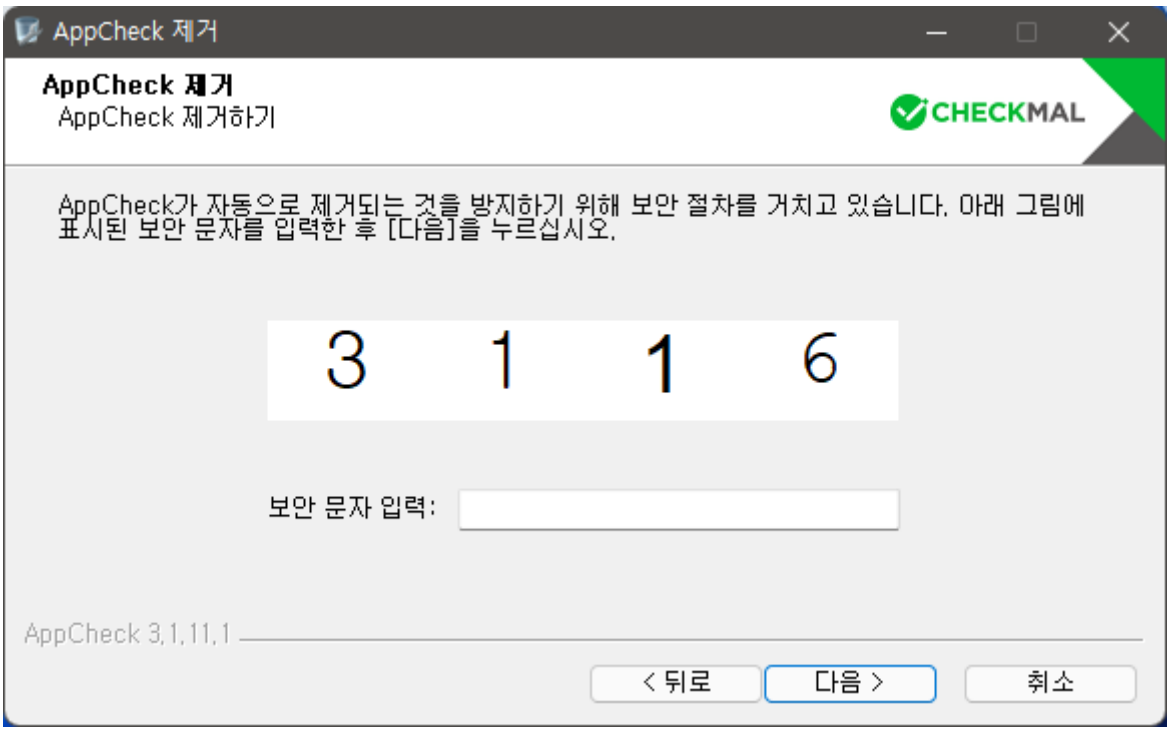
- **사용자가 임의로 삭제할 수 없습니다. 관리자에게 문의하시기 바랍니다. :** CMS 정책의 "어플리케이션 제거 허용" 항목이 체크 해제되어 있는 환경이다. AppCheck 제거를 위해서는 CMS 정책에서 "어플리케이션 제거 허용" 항목을 체크한 후 수정된 정책으로 에이전트 동기화가 적용된 후 제거하거나 또는 CMS 에이전트 리스트에서 삭제 대상 에이전트를 체크한 후 "에이전트 삭제" 메뉴를 이용하여 다음 라이브 체크 주기에 AppCheck 가 자동 삭제된다.

- **잠금이 설정되어 있어 삭제할 수 없습니다. 잠금 설정 해제 후 다시 시도하시기 바랍니다. :** "AppCheck 옵션 – 일반 – 잠금 설정 사용" 항목을 해제(비밀번호 2 회 입력 필요) 후 AppCheck 프로그램 삭제가 가능하다.

(2) 프로그램 제거를 위한 "AppCheck 제거를 시작합니다." 화면에서 "다음" 버튼을 클릭한다.

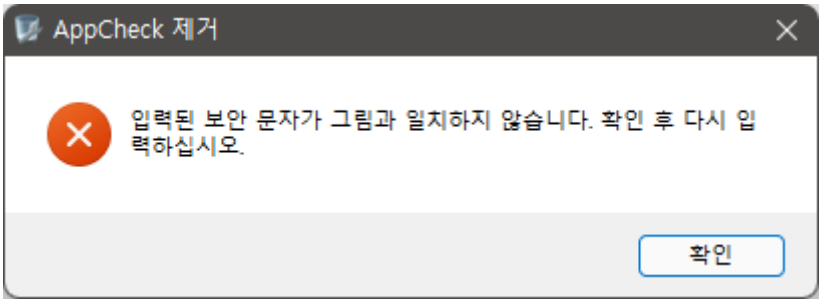


(3) AppCheck가 자동으로 제거되는 것을 방지하기 위한 보안 문자(CAPTCHA)를 확인하여 "보안 문자 입력" 란에 제시된 4자리 숫자를 입력한 후 "다음" 버튼을 클릭한다.

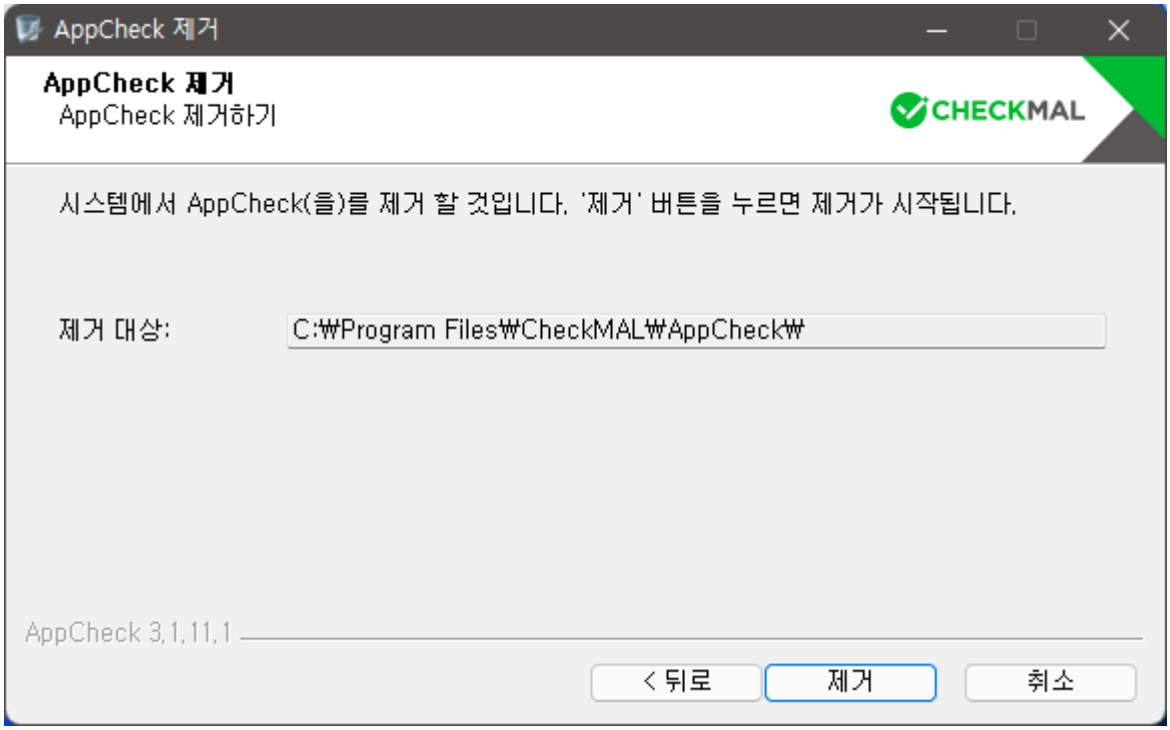


만약 잘못된 보안 문자를 입력한 경우 "입력된 보안 문자가 그림과 일치하지 않습니다. 확인 후

다시 입력하십시오." 메시지 창이 생성되므로 보안 문자를 다시 확인 후 입력한다.

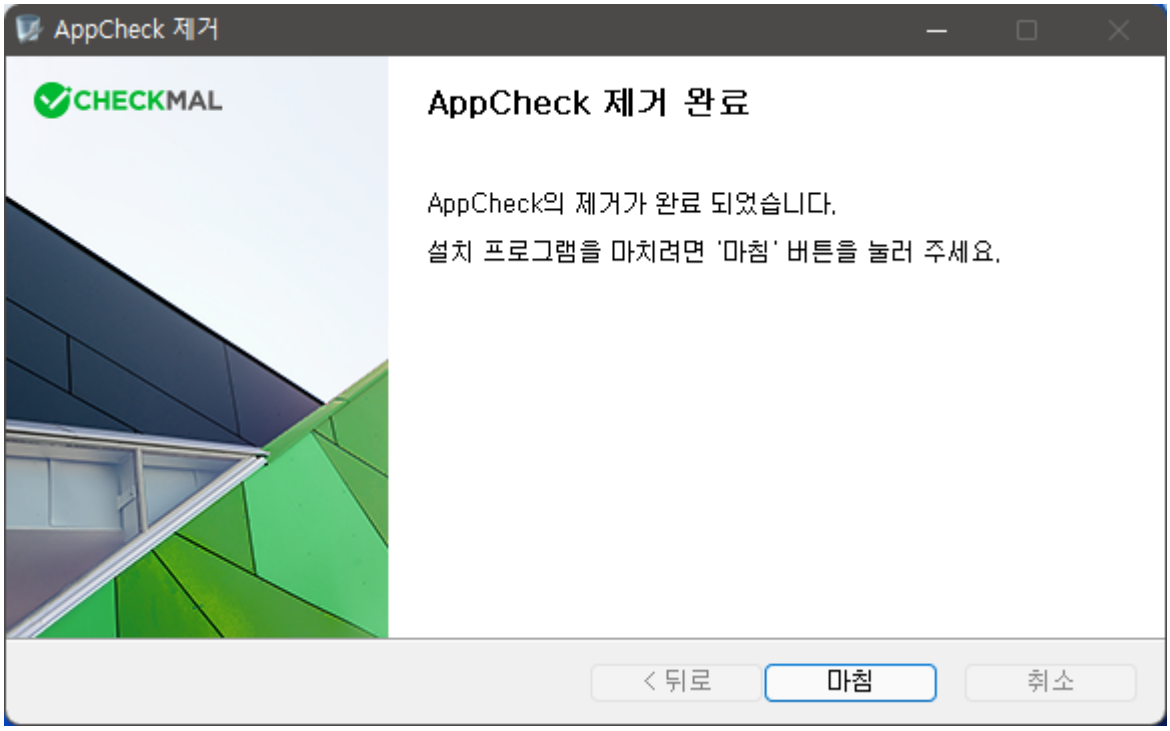


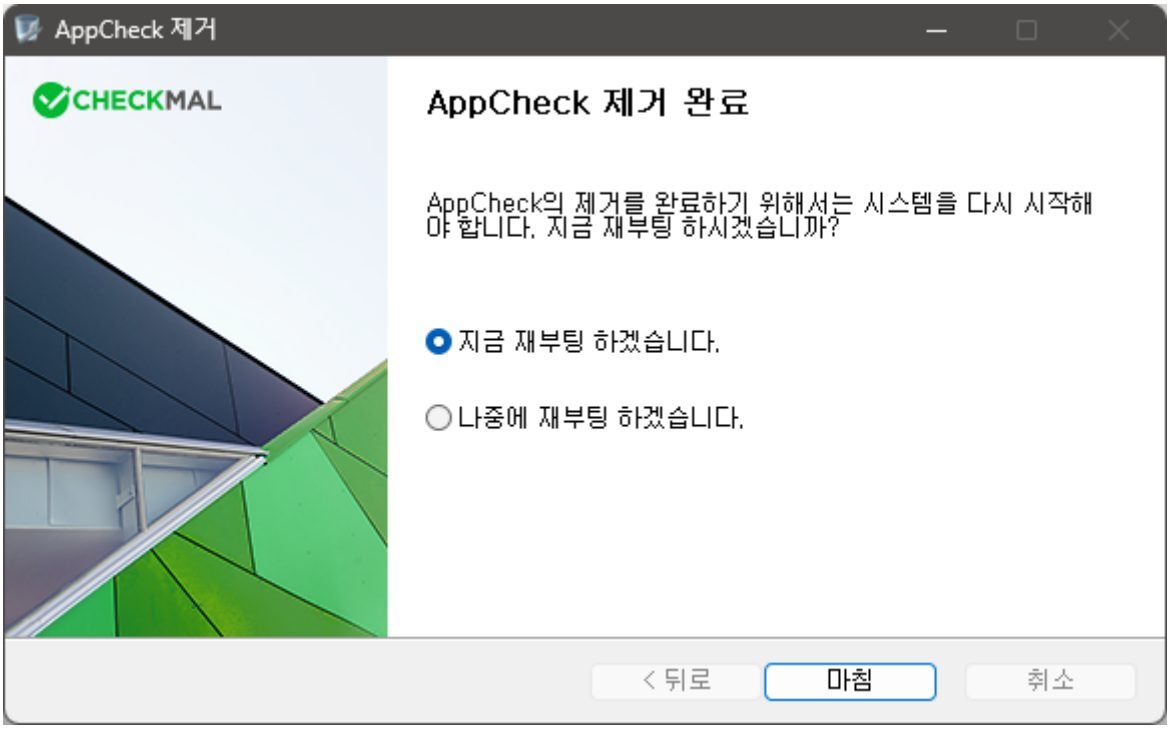
(4) 시스템에서 AppCheck를 제거하기 위해서는 "제거" 버튼을 클릭하며, 제거 대상은 "C:₩Program Files₩CheckMAL₩AppCheck" 폴더 전체와 "C:₩ProgramData₩CheckMAL₩AppCheck" 폴더 내 파일들이다. 단, "C:₩ProgramData₩CheckMAL₩AppCheck₩logs" 폴더는 프로그램 제거 후에도 유지된다.



만약 랜섬웨어 대피소 폴더 경로가 기본 경로 (C:₩ProgramData₩CheckMAL₩AppCheck₩RansomShelter)가 아닌 다른 경로로 지정되어 있는 경우 대피소 파일은 자동 삭제되지 않으므로 AppCheck 프로그램 제거 후 수동으로 삭제해야 한다.

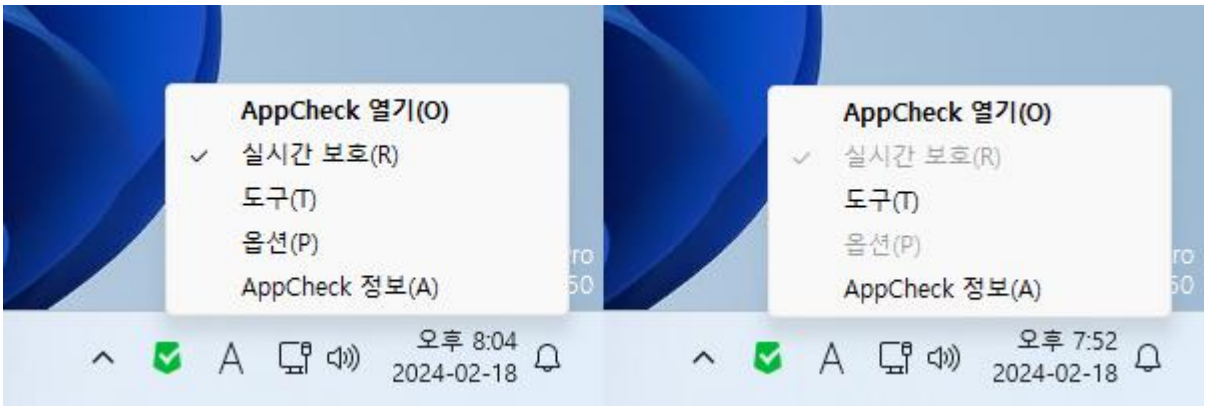
(5) AppCheck 제거가 완료된 후 "마침" 버튼을 클릭하면 프로그램 제거가 종료되며, 일부 시스템 환경에 따라서는 재부팅을 요구할 수 있다.





4. AppCheck : 아이콘 메뉴

작업 표시줄 알림 영역에 표시되는 AppCheck 아이콘 메뉴는 잠금 설정 사용 또는 CMS 중앙 관리 정책을 통한 Lock Mode 적용 시에는 실시간 보호와 옵션 메뉴가 비활성화 처리되어 변경할 수 없다.



⊙ **AppCheck 열기(O) :** AppCheck 대시보드 화면 실행

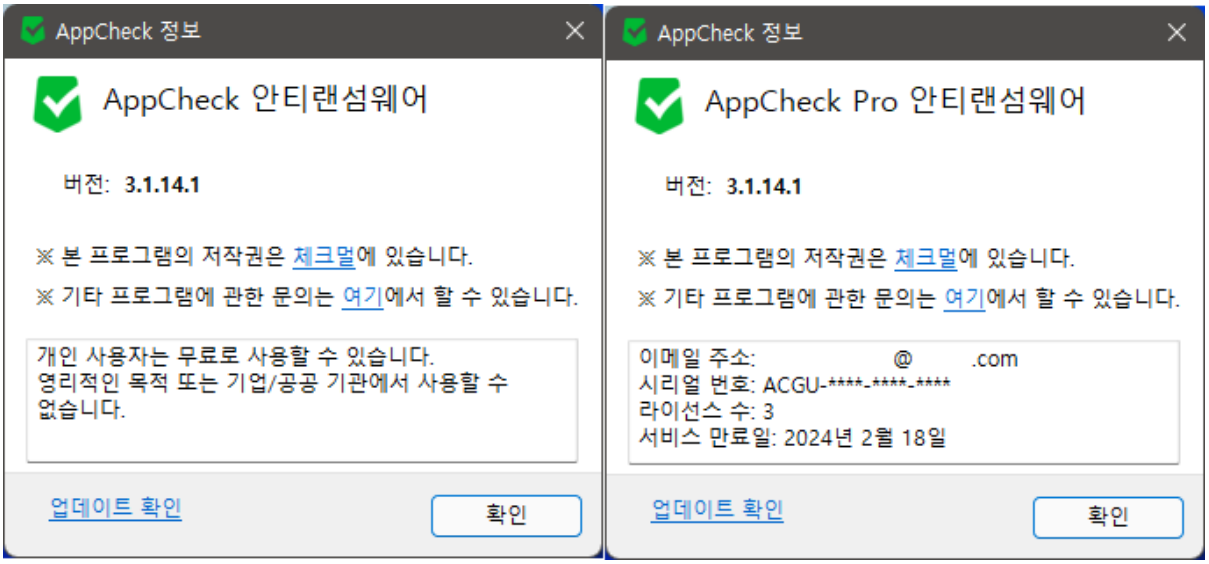
⊙ **실시간 보호(R) :** 랜섬웨어 행위 실시간 차단 및 롤백 (비)활성화 메뉴

- **녹색 아이콘 :** AppCheck 안티랜섬웨어 실시간 보호 중
- **회색 아이콘 :** AppCheck 안티랜섬웨어 실시간 보호 꺼짐

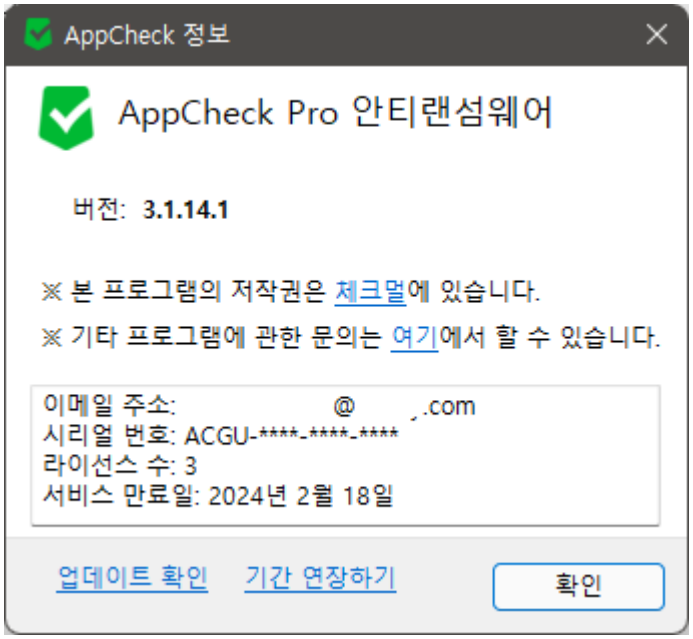
⊙ **도구(T) :** 일반 로그, 위협 로그, 검역소 화면 실행

⊙ **옵션(P) :** 일반, 랜섬 가드, 취약점 가드, 대피소, 자동 백업, 예외 설정, SMB 목록(AppCheck Pro 전용) 설정

⊙ **AppCheck 정보(A) :** AppCheck 버전, 저작권 및 프로그램 문의, 라이선스 안내, 정품 등록 정보(이메일 주소, 시리얼 번호, 라이선스 수, 서비스 만료일), 업데이트 확인

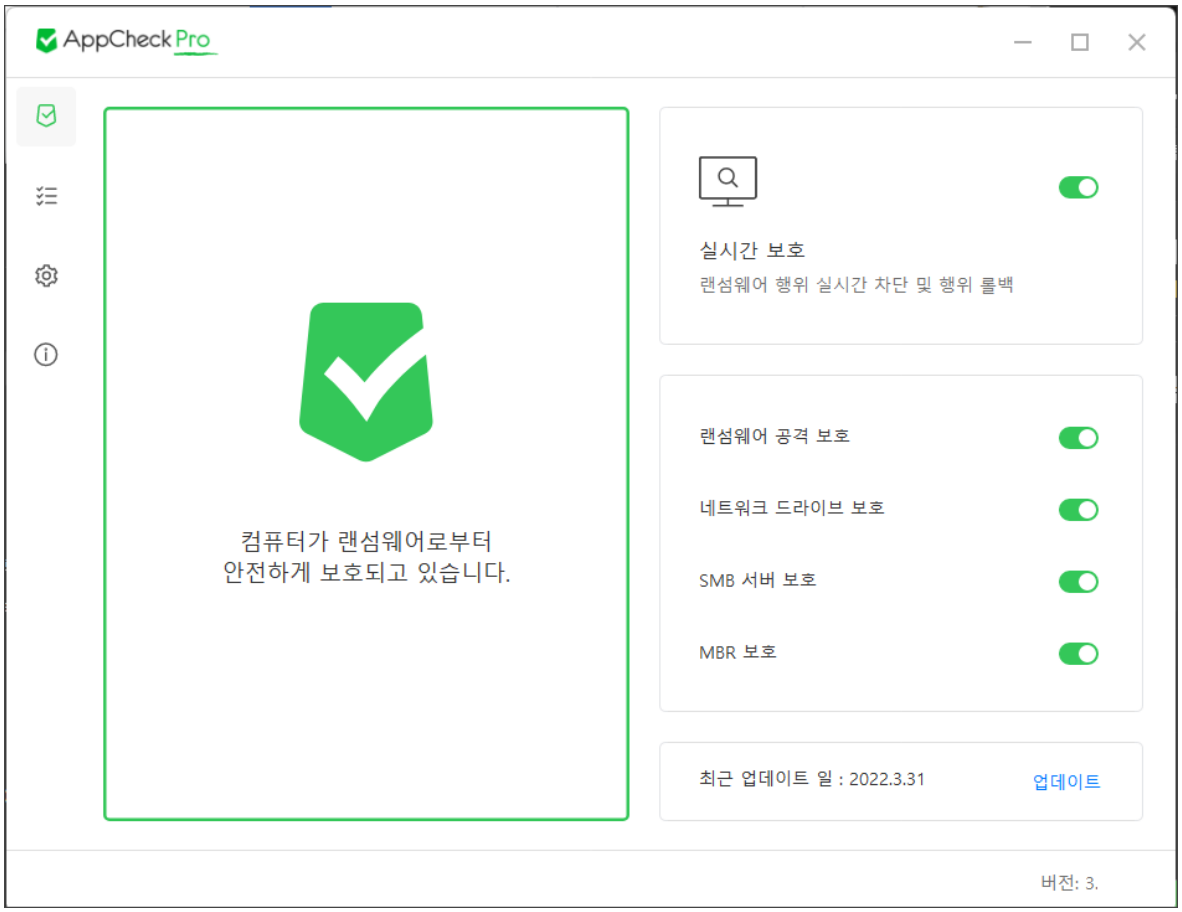


만약 AppCheck Pro 라이선스 만료일이 31 일 이내로 남은 경우 AppCheck 정보창에 "기간 연장하기" 메뉴를 자동 생성하여 클릭 시 체크멀 라이선스 갱신 페이지로 자동 연결되며, 라이선스 갱신이 이루어진 경우 기존에 사용하는 라이선스 정보 그대로 사용할 수 있다.



참고로 "기간 연장하기" 메뉴는 단독 설치형 버전에서 라이선스 만료 31 일 전부터 표시되며, CMS 중앙 관리를 통해 배포된 AppCheck Pro 안티랜섬웨어 제품에서는 표시되지 않는다.

5. AppCheck : 대시보드



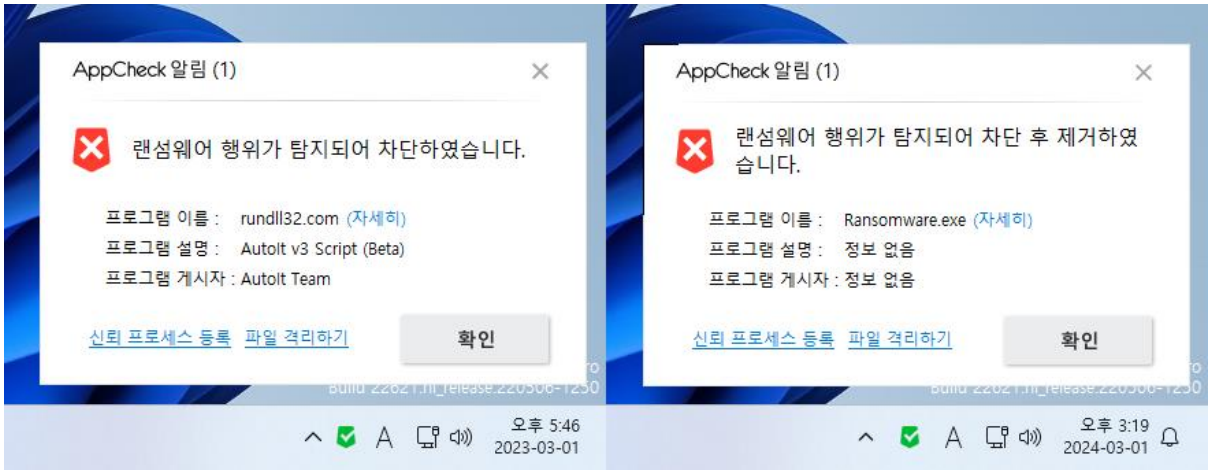
⊙ **실시간 보호**

- 활성화(ON) : 랜섬웨어 공격 보호, 네트워크 드라이브 보호, SMB 서버 보호, MBR 보호 중 1개 이상의 보호 기능이 활성화(ON)되어 있는 경우
- 비활성화(OFF) : 랜섬웨어 공격 보호, 네트워크 드라이브 보호, SMB 서버 보호, MBR 보호 모두 비활성화(OFF)된 경우

- **실시간 보호 중** : 컴퓨터가 랜섬웨어로부터 안전하게 보호되고 있습니다.
- **실시간 보호 꺼짐** : 컴퓨터가 랜섬웨어 위협에 노출되어 있습니다.

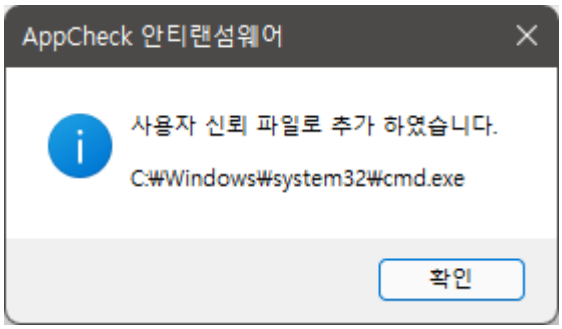
⊙ **랜섬웨어 공격 보호 :** 보호할 파일 확장명에 포함된 파일들이 탐지 조건에 따라 훼손될 경우 "랜섬웨어 행위 탐지" 또는 "랜섬웨어 행위 고급 탐지"를 통한 차단/제거 및 자동 복원 (비)활성화

랜섬웨어 공격 보호 (비)활성화 시 네트워크 드라이브 보호와 SMB 서버 보호도 함께 (비)활성화 처리되며, 네트워크 드라이브 보호 또는 SMB 서버 보호 기능 중 1개라도 활성화될 경우 랜섬웨어 공격 보호는 활성화된다.

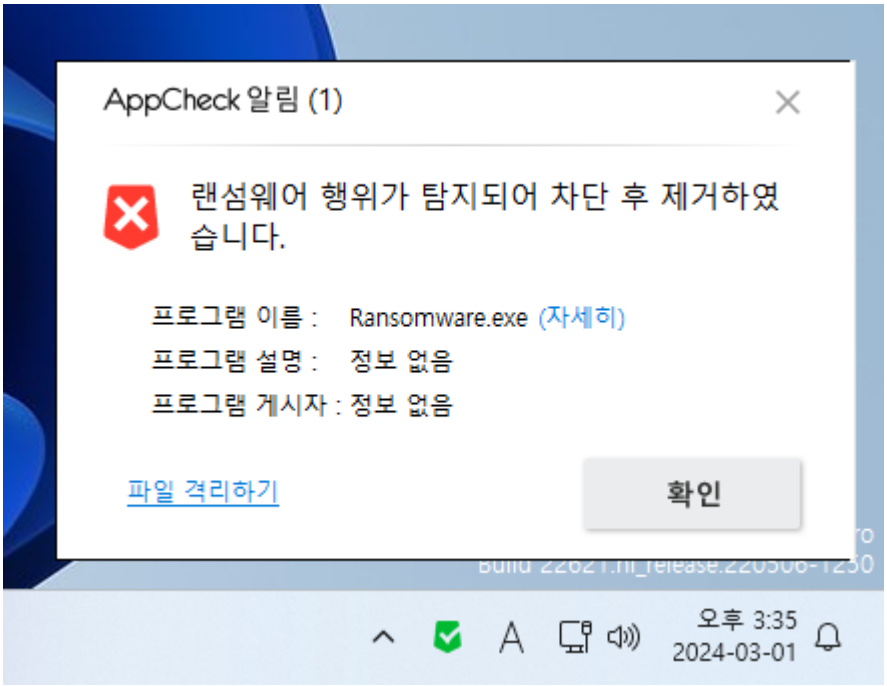


- **프로그램 이름 :** 파일 훼손 행위로 차단/제거된 파일명

- **프로그램 이름 (자세히) :** "도구 - 위협 로그" 메뉴로 자동 연결
- **프로그램 설명 :** 랜섬웨어 행위 탐지된 파일 속성에 표시된 파일 설명
- **프로그램 게시자 :** 랜섬웨어 행위 탐지된 파일의 디지털 서명 이름
- **신뢰 프로세스 등록 :** 랜섬웨어 행위로 탐지된 파일이 정상 프로그램 동작 중 탐지된 경우 "신뢰 프로세스 등록" 메뉴를 통해 "옵션 – 예외 설정 – 신뢰 프로세스 목록"에 자동 추가되어 예외 처리할 수 있으며, 등록 시 "사용자 신뢰 파일로 추가 하였습니다." 알림 메시지 창을 생성한다.

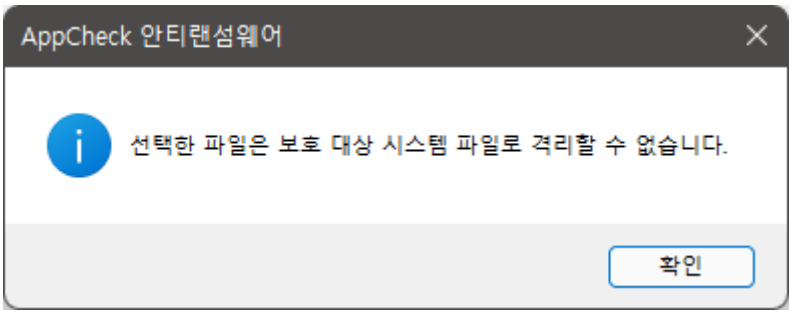


만약 잠금 설정 사용 또는 CMS 중앙 관리 정책의 "Lock Mode" 사용 환경에서는 랜섬웨어 행위 탐지 알림창에서 "신뢰 프로세스 등록" 메뉴가 표시되지 않는다.

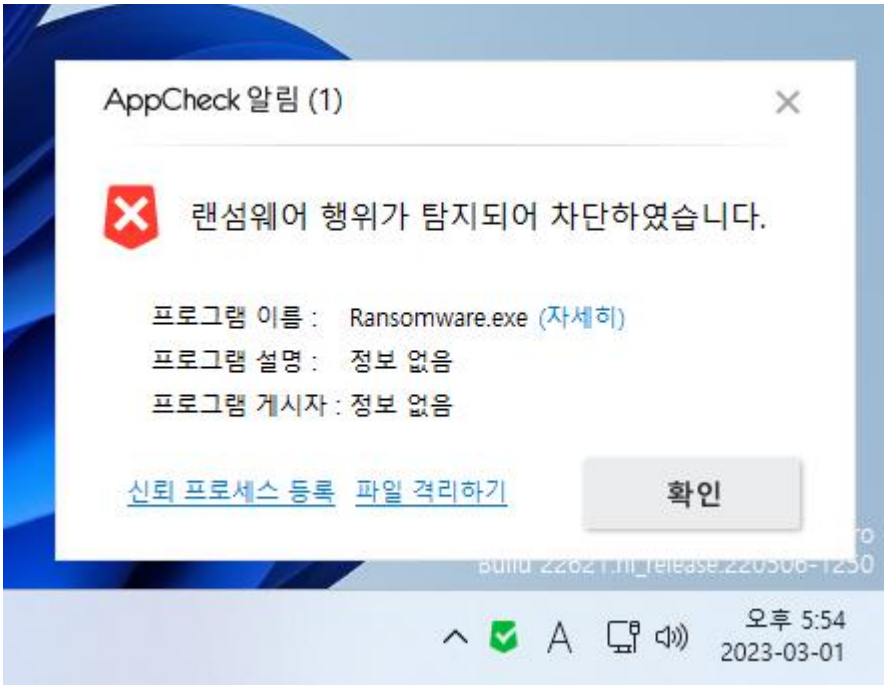


- **파일 격리하기 :** 랜섬웨어 행위로 탐지된 파일이 차단 후 제거에 실패할 경우 "파일 격리하기" 메뉴를 통해 검역소로 삭제 처리한다.

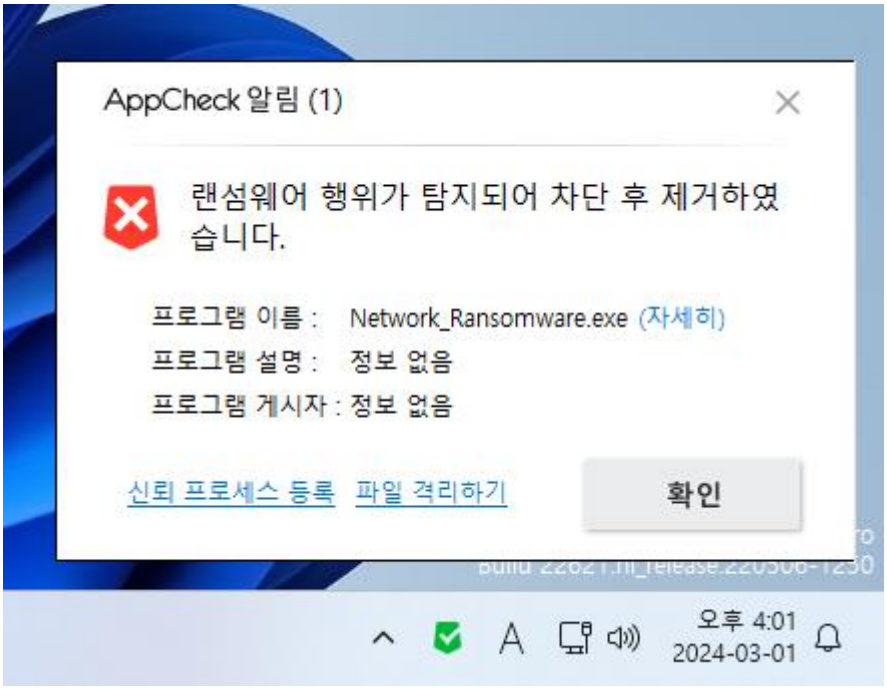
랜섬웨어 행위로 탐지된 파일 중 보호 대상 시스템 파일(※ 예시 : C:₩WINDOWS₩system32₩cmd.exe)로 인하여 자동 제거되지 않는 파일을 "파일 격리하기" 메뉴로 삭제를 시도할 경우 "선택한 파일은 보호 대상 시스템 파일로 격리할 수 없습니다." 알림 메시지 창을 생성한다.



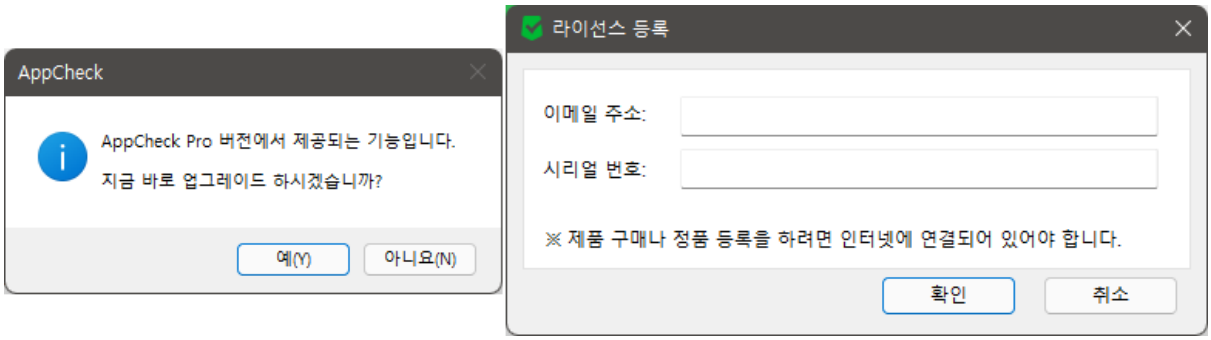
참고로 AppCheck 개인 사용자용 무료 버전에서는 랜섬웨어 행위로 탐지된 파일은 차단(종료)만 지원하며, AppCheck Pro 정품 버전에서는 차단 및 자동 치료(삭제) 기능을 제공한다.



⊙ **네트워크 드라이브 보호 :** AppCheck가 설치된 장치에서 네트워크 드라이브(SMB) 연결 방식으로 다른 저장 장치에 위치한 공유 폴더 내 파일들이 훼손될 경우 "랜섬웨어 행위 탐지"를 통한 차단/제거 및 자동 복원 (비)활성화 (AppCheck Pro 전용)

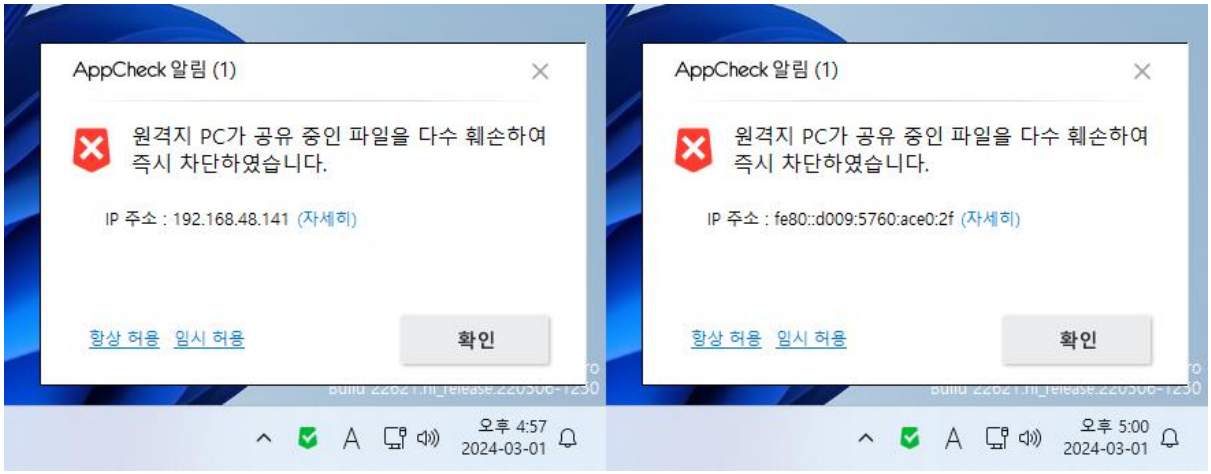


AppCheck 무료 버전에서 보호 기능 활성화 시 "AppCheck Pro 버전에서 제공되는 기능입니다. 지금 바로 업그레이드 하시겠습니까?" 알림 메시지 창이 생성된다.

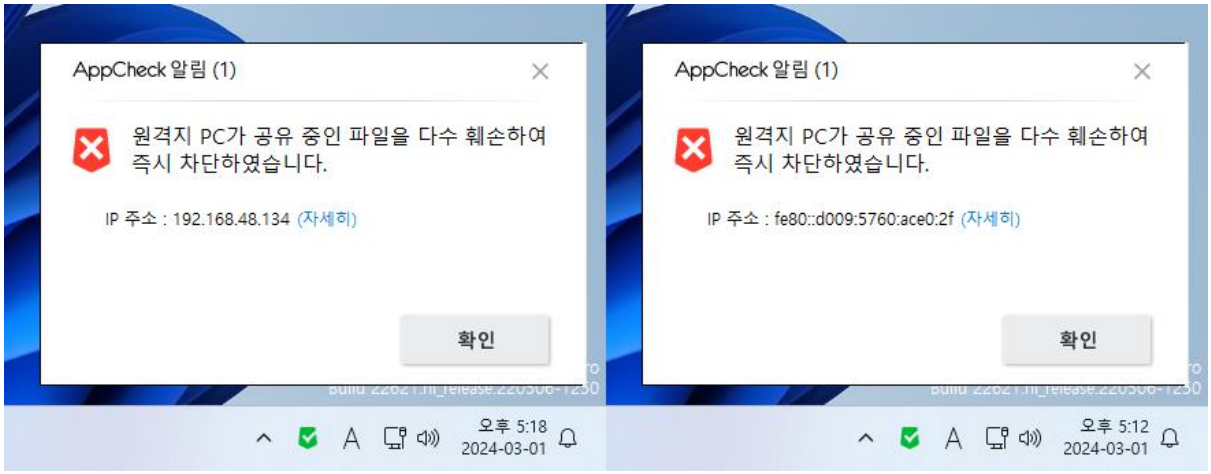


"예(Y)" 버튼 클릭 시 구입한 AppCheck Pro 라이선스 정보(이메일 주소, 시리얼 번호)를 입력하면 AppCheck Pro 정품 버전으로 변경되며 정품 등록 시에는 반드시 인터넷 연결이 필요하다.

⊙ **SMB 서버 보호 :** 원격지 PC에서 실행된 랜섬웨어가 네트워크 드라이브(SMB)로 연결된 공유 폴더 내 파일들을 훼손할 경우 공유 폴더가 존재하는 장치에 설치된 AppCheck Pro가 원격지 IP 주소를 1시간 동안 임시 차단 및 자동 복원 (비)활성화 (AppCheck Pro 전용)

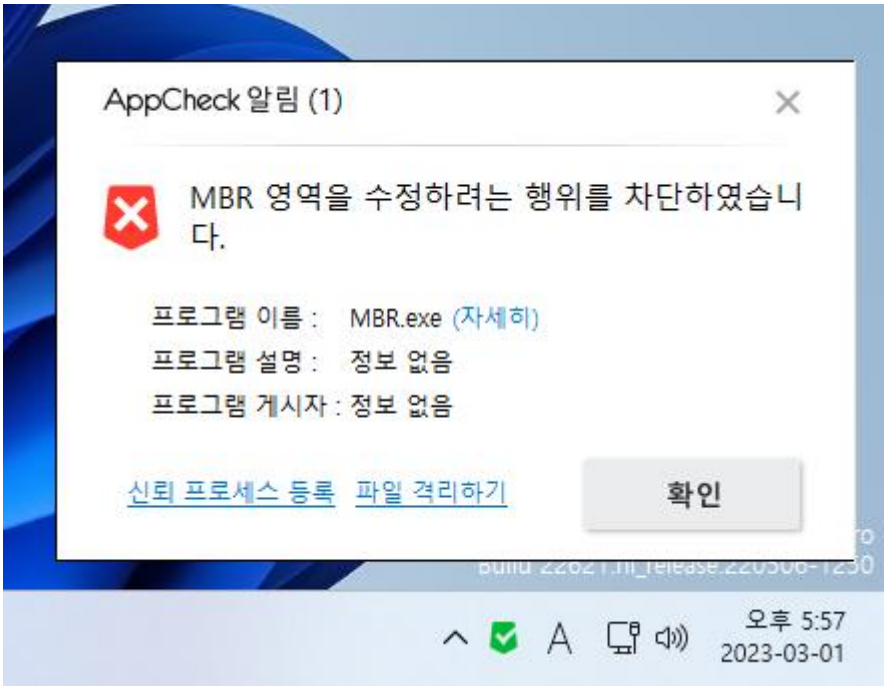


만약 잠금 설정 사용 또는 CMS 중앙 관리 정책의 "Lock Mode" 사용 환경에서는 원격지 PC의 IP 주소 차단 알림창에서 "항상 허용"과 "임시 허용" 메뉴가 표시되지 않는다.

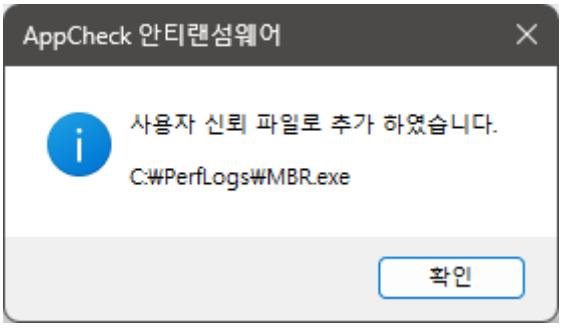


⊙ **MBR 보호 :** Master Boot Record (MBR) 영역의 변조를 시도하는 파일 실행 차단 (비)활성화

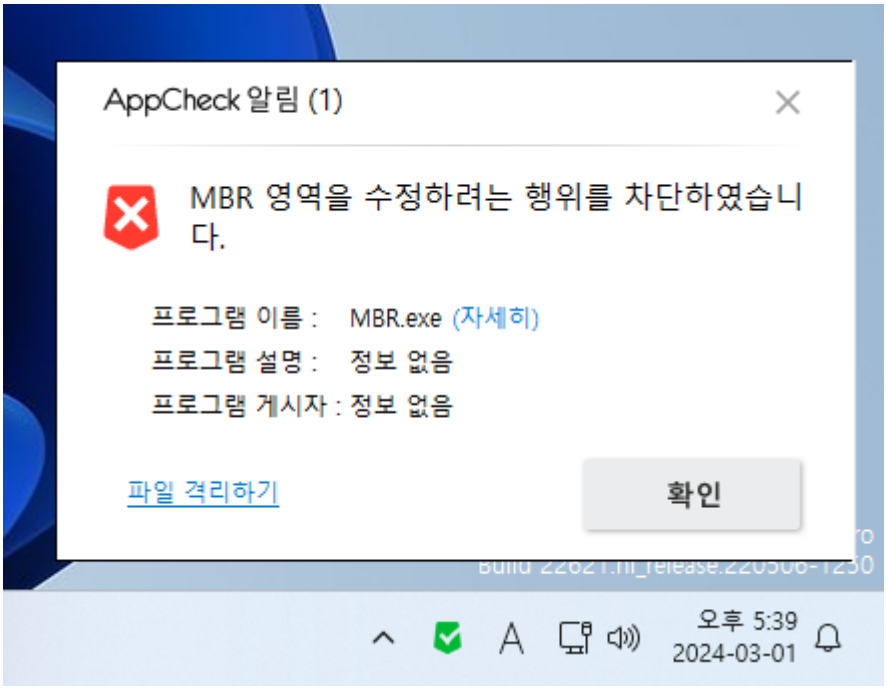
MBR 보호 기능을 통한 탐지는 탐지된 파일을 차단(종료)하며, 두 번째 재실행 시부터는 랜섬웨어 행위 탐지로 제거된다.



- **프로그램 이름 :** MBR 영역 훼손 행위로 차단된 파일명
- **프로그램 이름 (자세히) :** "도구 - 위협 로그" 메뉴로 자동 연결
- **프로그램 설명 :** MBR 영역 훼손 행위로 차단된 파일 속성에 표시된 파일 설명
- **프로그램 게시자 :** MBR 영역 훼손 행위로 차단된 파일의 디지털 서명 이름
- **신뢰 프로세스 등록 :** MBR 보호 기능으로 차단된 파일이 정상 프로그램 동작 중 차단된 경우 "신뢰 프로세스 등록" 메뉴를 통해 "옵션 – 예외 설정 – 신뢰 프로세스 목록"에 자동 추가되어 예외 처리할 수 있으며, 등록 시 "사용자 신뢰 파일로 추가 하였습니다." 알림 메시지 창을 생성한다.



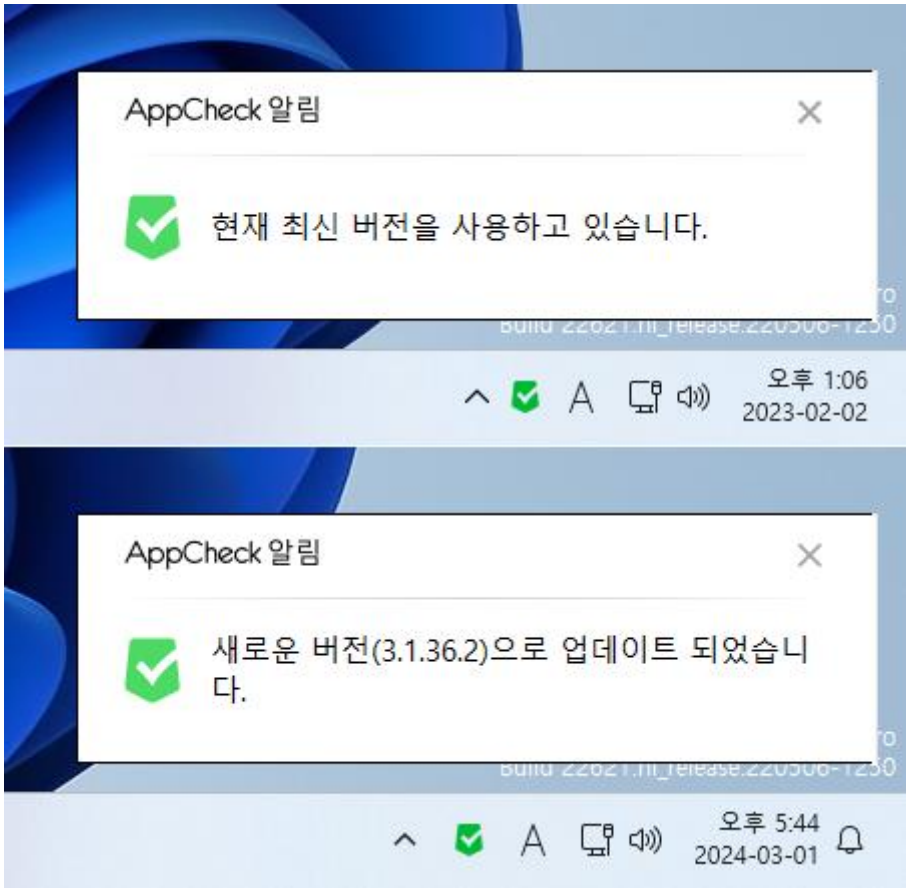
만약 잠금 설정 사용 또는 CMS 중앙 관리 정책의 "Lock Mode" 사용 환경에서는 MBR 차단 알림 창에서 "신뢰 프로세스 등록" 메뉴가 표시되지 않는다.



- **파일 격리하기 :** MBR 보호 기능으로 차단된 파일이 악성 파일인 경우 "파일 격리하기" 메뉴를 통해 검역소로 삭제 처리한다.

⊙ **최근 업데이트 일 :** AppCheck 자동(수동) 업데이트를 통해 마지막 발드 버전 업데이트가 이루어진 날짜

업데이트 메뉴를 클릭 시 최신 빌드 버전 환경에서 "현재 최신 버전을 사용하고 있습니다." 알림 메시지가 생성되며, 구 빌드 버전 환경에서는 최신 빌드 버전으로 자동 업데이트가 진행된 후 "새로운 버전(3.1.○.○)으로 업데이트 되었습니다." 알림 메시지가 생성된다.


AppCheck 알림
현재 최신 버전을 사용하고 있습니다.
오후 1:06
2023-02-02
AppCheck 알림
새로운 버전(3.1.36.2)으로 업데이트 되었습니다.
오후 5:44
2024-03-01

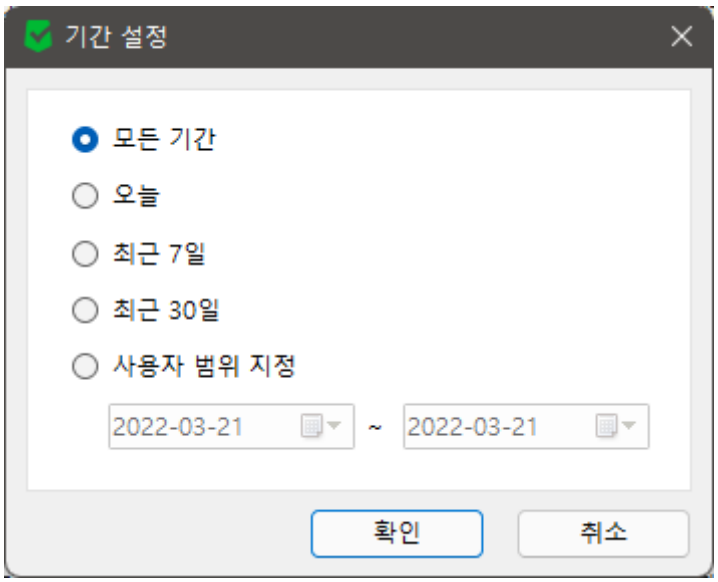
6. AppCheck : 도구

[6-1] 일반 로그

일반 로그는 최근 30일(기본값) 동안 AppCheck 동작 중 발생하는 검역소, 세션 프로그램, 서비스 프로그램, 업데이트, 알림 메시지, 자동 백업 등 다양한 정보를 표시한다.

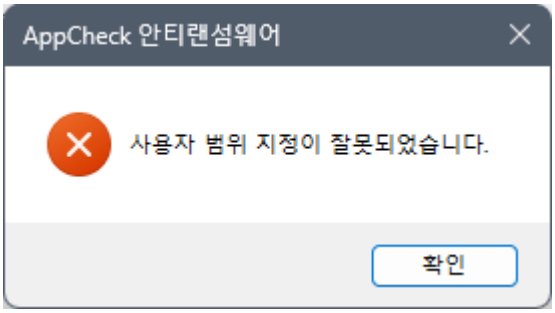
일반 로그의 칼럼(Columns)은 날짜, 수준, 구분, 내용으로 구분되며, 각 항목별 내림차순/오름차순으로 정렬할 수 있다.

일반 로그의 "기간 설정" 메뉴를 통해 지정한 특정 기간 내에 기록된 일반 로그 내역을 필터링하여 확인할 수 있다.

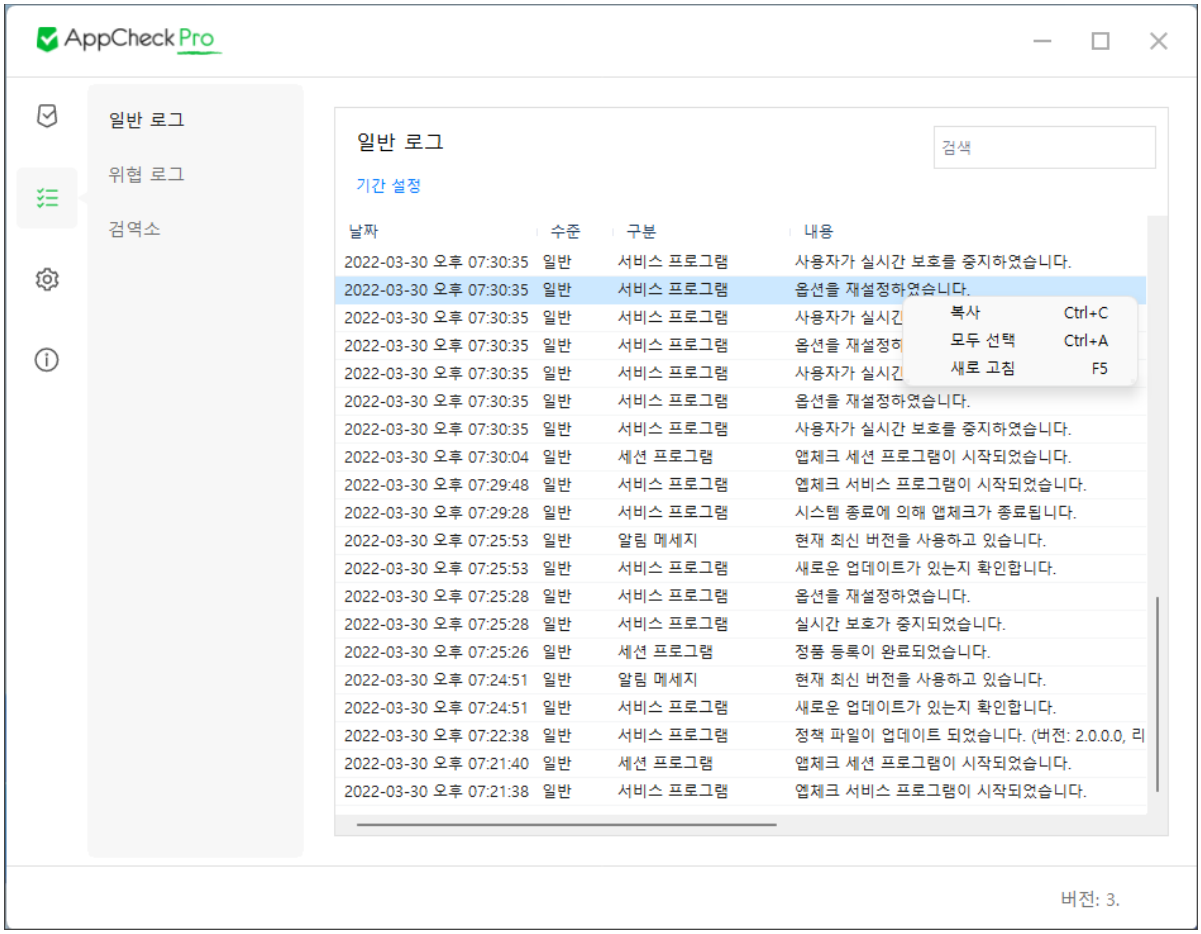


- **모든 기간 :** 모든 기간 동안의 일반 로그 확인
- **오늘 :** 오늘 날짜 기준으로 기록된 일반 로그 확인
- **최근 7일 :** 최근 7일 기준으로 기록된 일반 로그 확인
- **최근 30일 :** 최근 30일 기준으로 기록된 일반 로그 확인
- **사용자 범위 지정 :** 특정 기간(년-월-일 지정) 동안에 기록된 일반 로그 확인

"사용자 범위 지정" 시 유효하지 않은 날짜 범위로 설정할 경우 "사용자 범위 지정이 잘못되었습니다." 알림 메시지 창이 생성된다.



일반 로그에 기록된 특정 항목을 선택하여 마우스 우클릭 메뉴를 통해 복사, 모두 선택, 새로 고침을 할 수 있다.

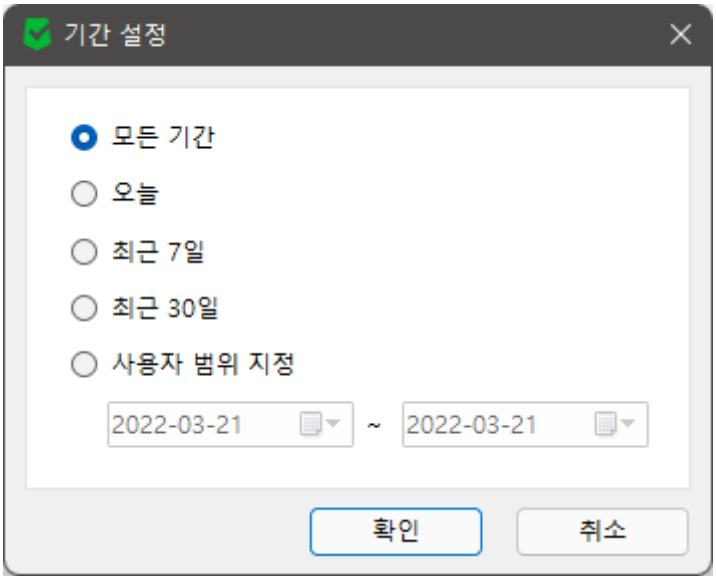


- **복사 (Ctrl+C) :** 선택한 항목의 일반 로그 세부 정보 복사하기
- **모두 선택 (Ctrl+A) :** 일반 로그에 기록된 모든 항목 일괄 선택하기
- **새로 고침 (F5) :** 일반 로그에 기록된 정보 갱신

[6-2] 위협 로그

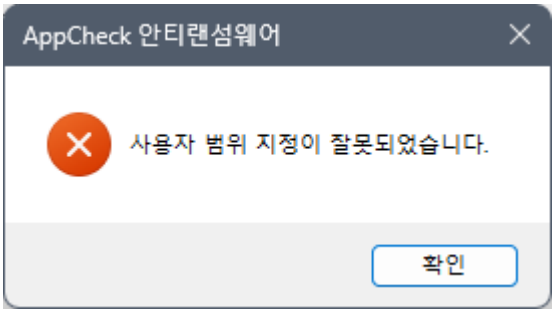
위협 로그는 최근 30일(기본값) 동안 랜섬 가드, 취약점 가드, MBR 보호 기능을 통해 탐지된 내역(차단, 제거, 복원, 제거 실패, 복원 실패) 정보를 표시한다.

위협 로그의 "기간 설정" 메뉴를 통해 지정한 특정 기간 내에 기록된 위협 로그 내역을 필터링하여 확인할 수 있다.

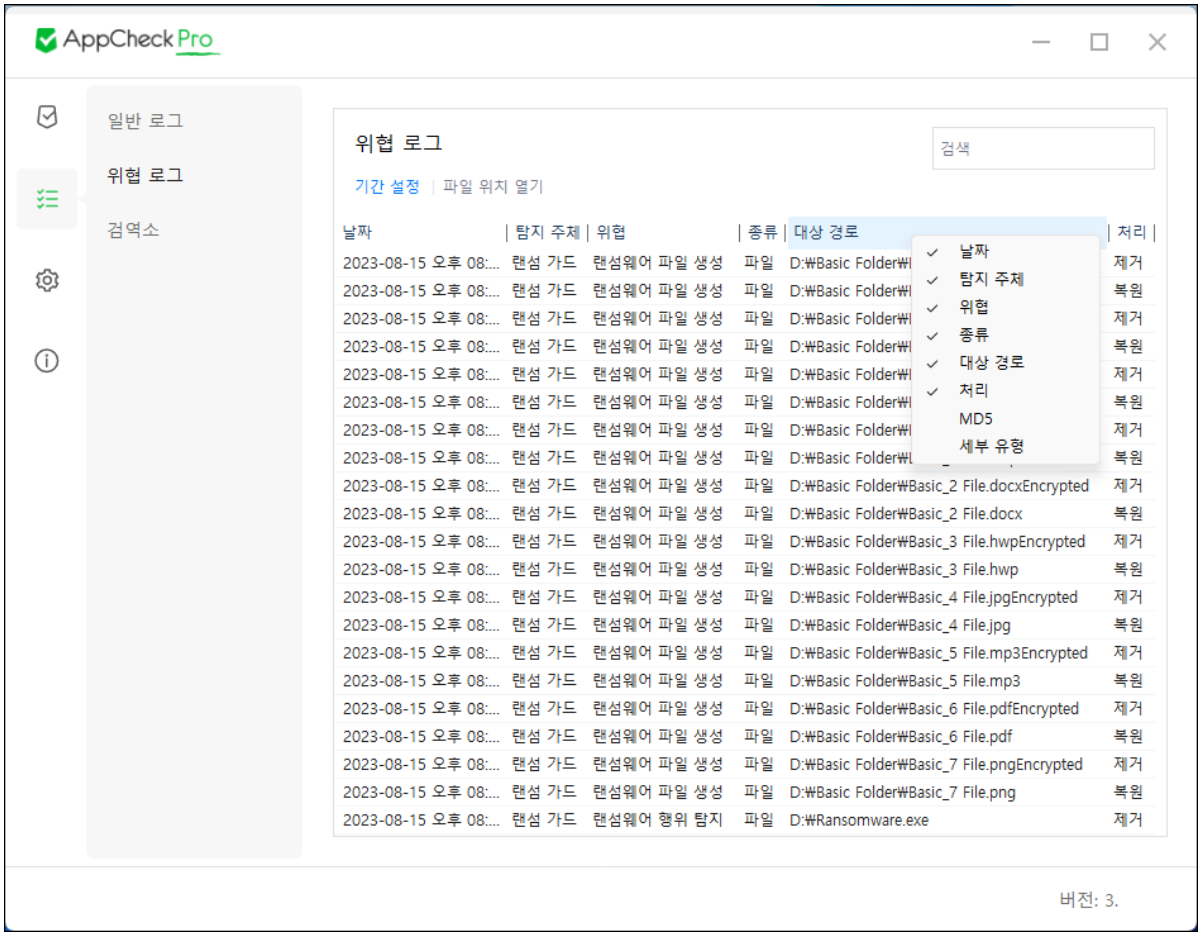


- **모든 기간 :** 모든 기간 동안의 위협 로그 확인
- **오늘 :** 오늘 날짜 기준으로 기록된 위협 로그 확인
- **최근 7일 :** 최근 7일 기준으로 기록된 위협 로그 확인
- **최근 30일 :** 최근 30일 기준으로 기록된 위협 로그 확인
- **사용자 범위 지정 :** 특정 기간(년-월-일 지정) 동안에 기록된 위협 로그 확인

"사용자 범위 지정" 시 유효하지 않은 날짜 범위로 설정할 경우 "사용자 범위 지정이 잘못되었습니다." 알림 메시지 창이 생성된다.

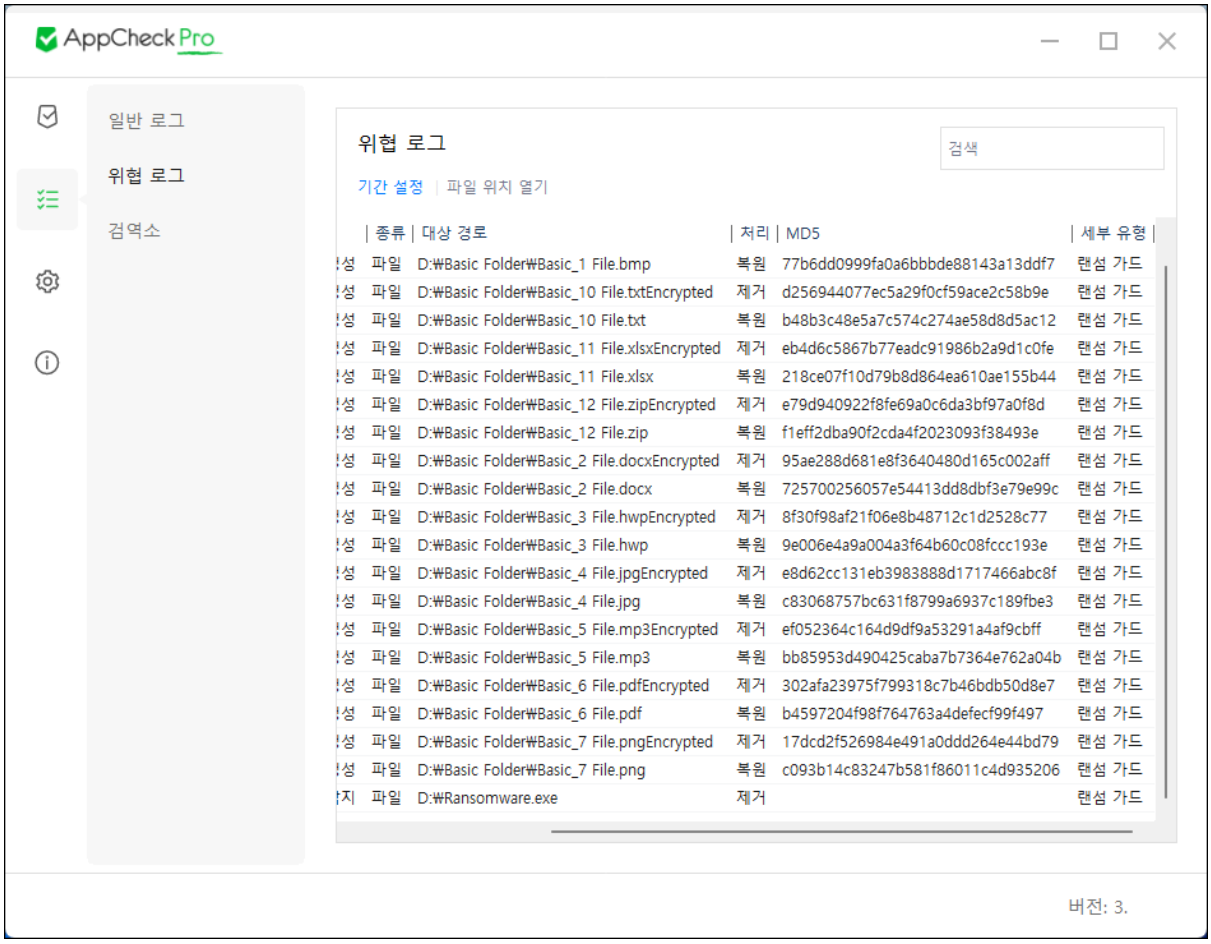


위협 로그의 칼럼(Columns)은 날짜, 탐지 주체, 위협, 종류, 대상 경로, 처리, MD5(기본값 : 비활성화), 세부 유형(기본값 : 비활성화)로 구분되며, 각 항목별 내림차순/오름차순으로 정렬할 수 있다.



- **차단 :** 랜섬웨어 행위로 탐지된 보호 대상 시스템 파일, MBR 보호로 탐지된 파일, IP 주소, 취약점 가드로 탐지된 응용 프로그램을 차단한다.
- **제거 :** 랜섬웨어 행위 탐지 및 랜섬웨어 행위 고급 탐지로 제거된 파일, 랜섬웨어에 의해 훼손된 파일 및 생성된 파일을 자동 삭제하여 검역소에 백업한다. 단, 위협 로그에서 제거로 표시된 파일 중에는 이미 삭제되어 존재하지 않는 파일도 포함된다.
- **복원 :** 랜섬웨어 대피소에 임시 백업된 파일을 이용하여 원래 위치로 복원한다.
- **제거 실패 :** 랜섬웨어 행위 탐지 시 제거해야 할 파일이 이미 삭제되어 존재하지 않거나 권한 문제 등으로 제거하지 못하는 경우에 기록한다.
- **복원 실패 :** 복원 대상 파일의 경로가 존재하지 않는 경우, 랜섬웨어 대피소에 임시 백업된 파일이 존재하지 않는 경우, 원본 파일 경로가 삭제되어 복원이 이루어지지 않은 경우에 기록한다.

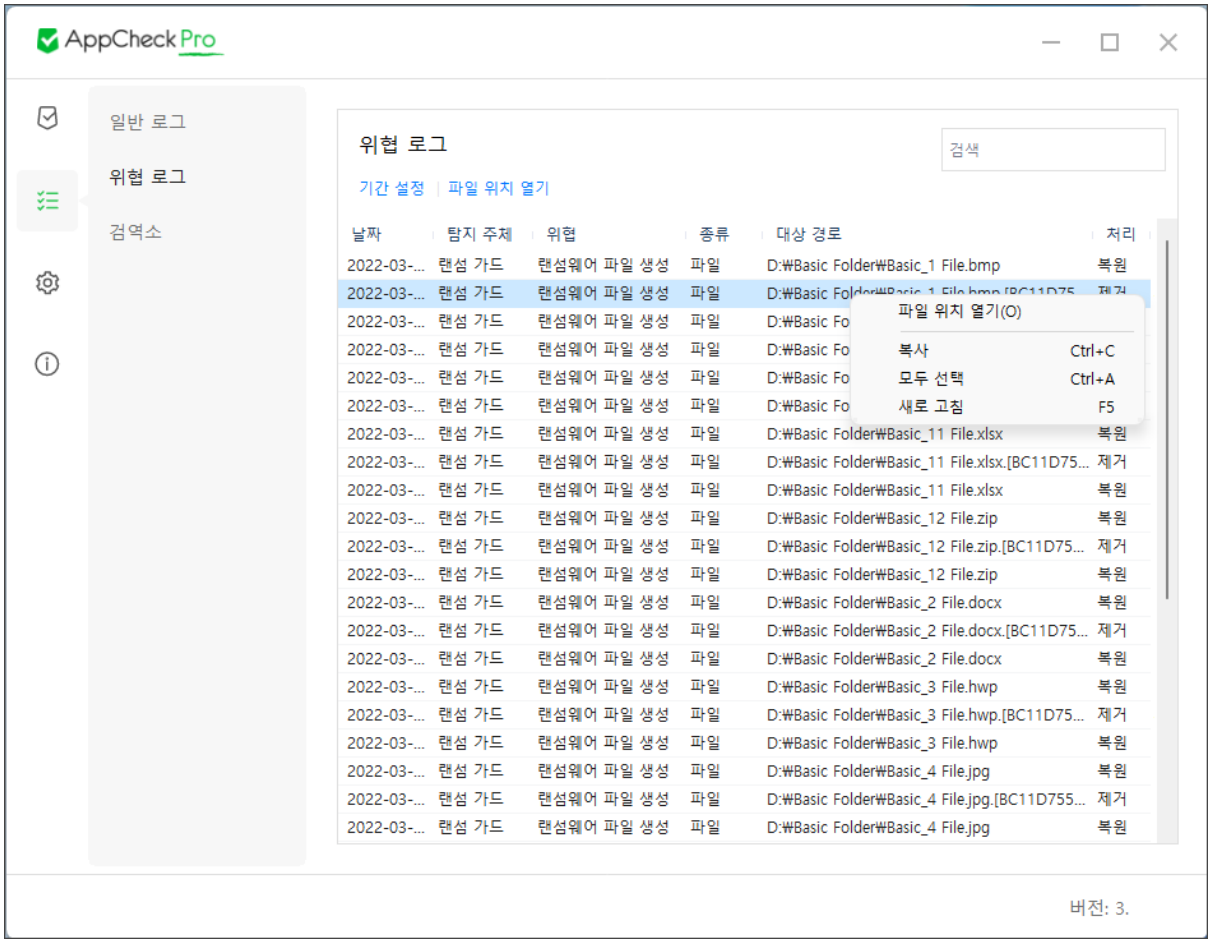
위협 로그에 기록된 항목에 대하여 MD5, 세부 유형 칼럼을 선택할 경우 해당 항목의 추가적인 정보를 확인할 수 있다.



- **MD5 :** 위협 로그에 기록된 파일에 대한 MD5값을 확인할 수 있다. 단, 일부 파일은 MD5값이 표시되지 않을 수 있으며 제거된 파일은 검역소에서 MD5값을 확인할 수 있다.

- **세부 유형 :** 탐지된 파일의 세부 유형을 N/A(MBR 변조 및 취약점 탐지), 랜섬 가드(랜섬웨어 행위 탐지, 네트워크 드라이브 보호), 고스트 탐지(랜섬웨어 행위 고급 탐지), 스마트 탐지(랜섬웨어 행위 고급 탐지), 시스템 위협(시스템 위협 탐지), SMB(SMB 서버 보호)로 표시한다.

위협 로그에 기록된 특정 항목을 선택하여 마우스 우클릭 메뉴를 통해 파일 위치 열기, 복사, 모두 선택, 새로 고침을 할 수 있다.

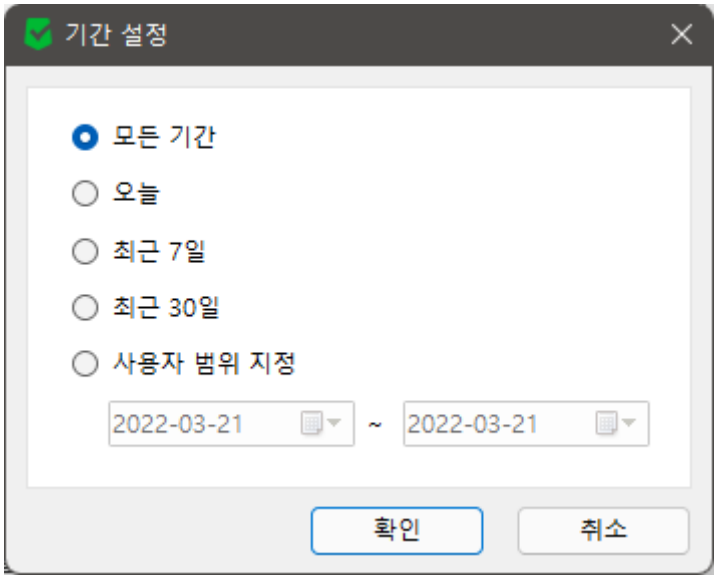


- **파일 위치 열기 :** Windows 탐색기를 이용하여 선택한 파일의 대상 경로 열기
- **복사 (Ctrl+C) :** 선택한 항목의 위협 로그 세부 정보 복사하기
- **모두 선택 (Ctrl+A) :** 위협 로그에 기록된 모든 항목 일괄 선택하기
- **새로 고침 (F5) :** 위협 로그에 기록된 정보 갱신

[6-3] 검역소

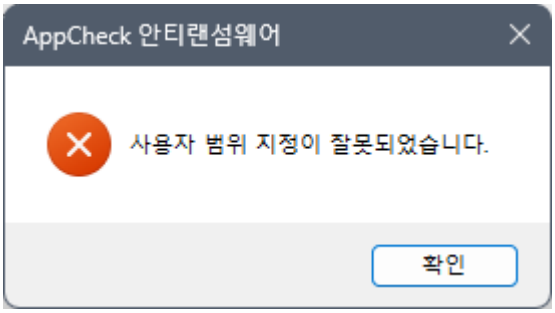
검역소는 최근 30일(기본값) 동안 랜섬웨어 행위 탐지를 통해 제거 처리되어 검역소 폴더(C:₩ProgramData₩CheckMAL₩AppCheck₩Quarantine)에 백업된 파일 정보를 제공하며, 필요에 따라 사용자가 검역소에 백업된 항목을 복원 및 삭제할 수 있다.

검역소의 "기간 설정" 메뉴를 통해 지정한 특정 기간 내에 기록된 검역소 로그를 필터링하여 확인할 수 있다.

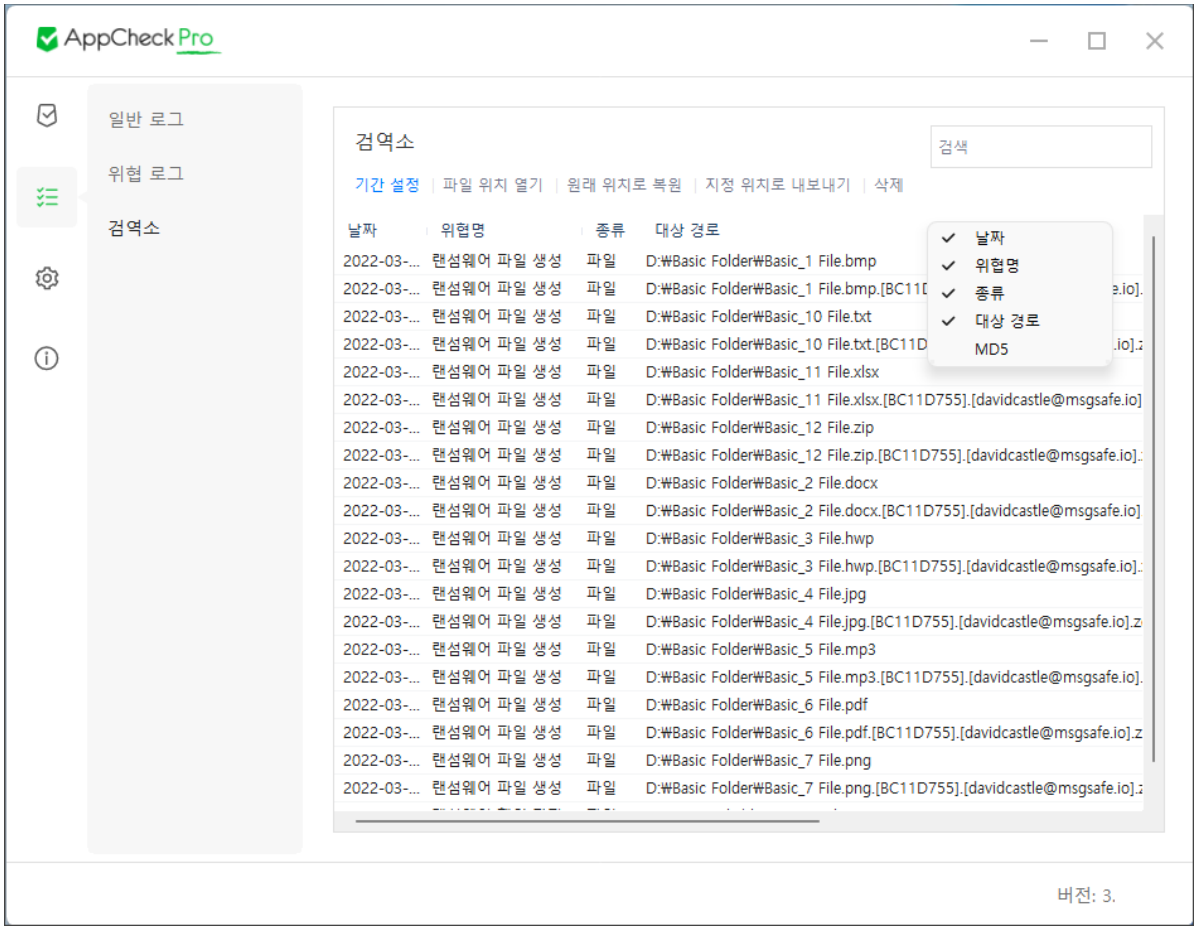


- **모든 기간 :** 모든 기간 동안의 검역소 로그 확인
- **오늘 :** 오늘 날짜 기준으로 기록된 검역소 로그 확인
- **최근 7일 :** 최근 7일 기준으로 기록된 검역소 로그 확인
- **최근 30일 :** 최근 30일 기준으로 기록된 검역소 로그 확인
- **사용자 범위 지정 :** 특정 기간(년-월-일 지정) 동안에 기록된 검역소 로그 확인

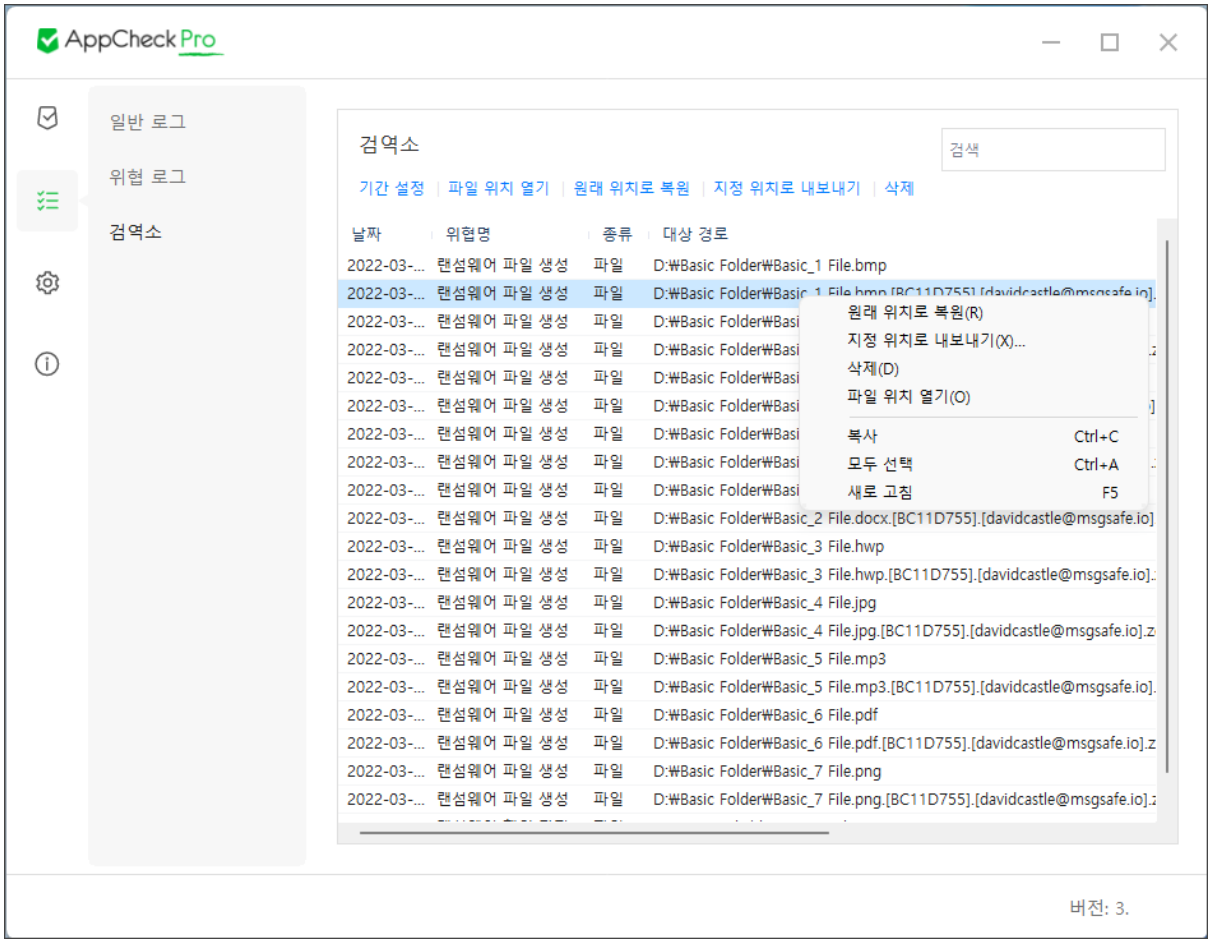
"사용자 범위 지정" 시 유효하지 않은 날짜 범위로 설정할 경우 "사용자 범위 지정이 잘못되었습니다." 알림 메시지 창이 생성된다.



검역소의 칼럼(Columns)은 날짜, 위협명, 종류, 대상 경로, MD5(기본값 : 비활성화)로 구분되며, 각 항목별 내림차순/오름차순으로 정렬할 수 있다.

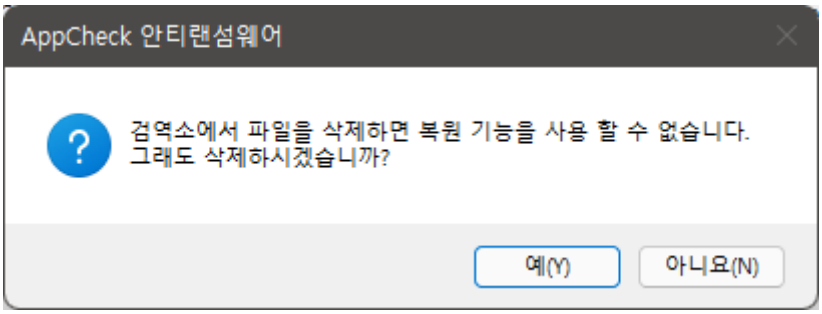


검역소에 기록된 특정 항목을 선택하여 마우스 우클릭 메뉴를 통해 파일 위치 열기, 복사, 모두 선택, 새로 고침을 할 수 있다.



- **원래 위치로 복원 :** 검역소에 백업된 선택 파일을 원래 위치(대상 경로)로 복원하기
- **지정 위치로 내보내기 :** 검역소에 백업된 선택 파일을 사용자가 지정한 폴더로 내보내기
- **삭제 :** 검역소에 백업된 파일 삭제하기

검역소에 백업된 파일 삭제 시 "검역소에서 파일을 삭제하면 복원 기능을 사용할 수 없습니다. 그래도 삭제하시겠습니까?" 메시지 창이 생성된다.되며, 삭제된 파일은 휴지통으로 이동하지 않고 완전히 삭제 처리된다.



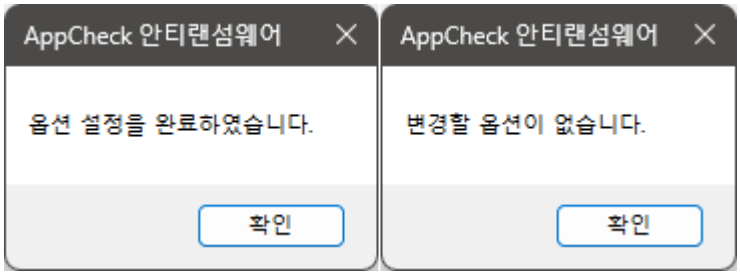
또한 검역소 삭제 메뉴를 통해 삭제된 후에는 해당 파일에 대한 검역소 로그도 삭제된다.

- **파일 위치 열기 :** Windows 탐색기를 이용하여 선택한 파일이 존재했던 위치(대상 경로) 열기
- **복사 (Ctrl+C) :** 선택한 항목의 검역소 로그 세부 정보 복사하기
- **모두 선택 (Ctrl+A) :** 검역소 로그에 기록된 모든 항목 일괄 선택하기
- **새로 고침 (F5) :** 검역소 로그에 기록된 정보 갱신

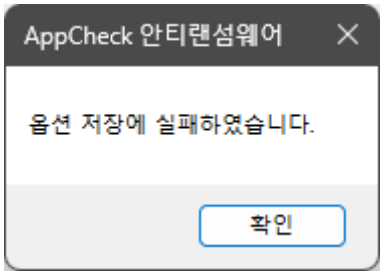
7. AppCheck : 옵션

AppCheck 옵션은 일반, 랜섬 가드, 취약점 가드, 대피소, 자동 백업, 예외 설정, SMB 목록으로 구성되어 있다.

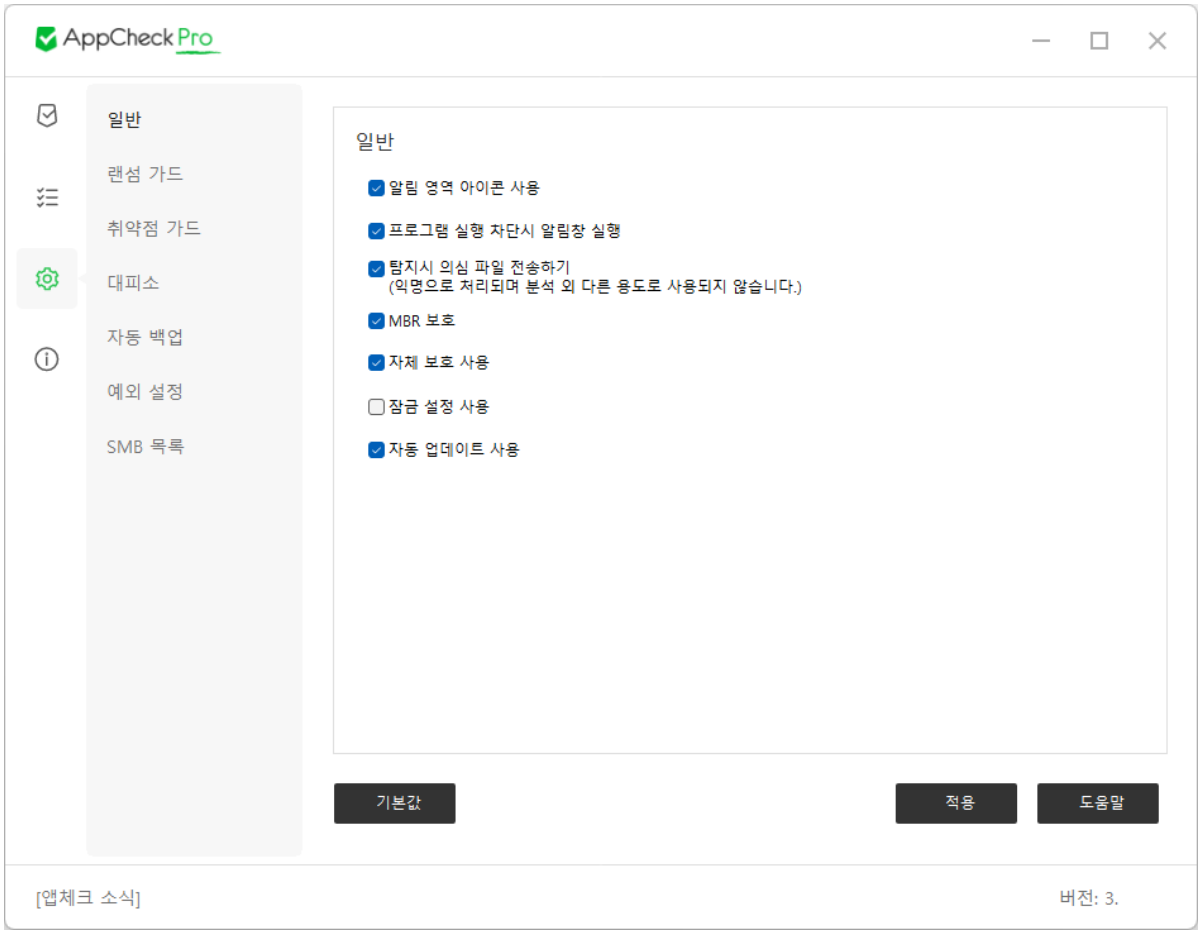
AppCheck 옵션 설정을 변경한 후 "적용" 버튼 클릭 시 "옵션 설정을 완료하였습니다." 안내 메시지 창이 생성되며, 옵션 설정 변경없이 "적용" 버튼 클릭 시 "변경할 옵션이 없습니다." 안내 메시지 창이 생성된다.



AppCheck 옵션 설정 후 적용 시 유효하지 않은 설정인 경우 "옵션 저장에 실패하였습니다." 안내 메시지 창이 생성된다.



[7-1] 일반



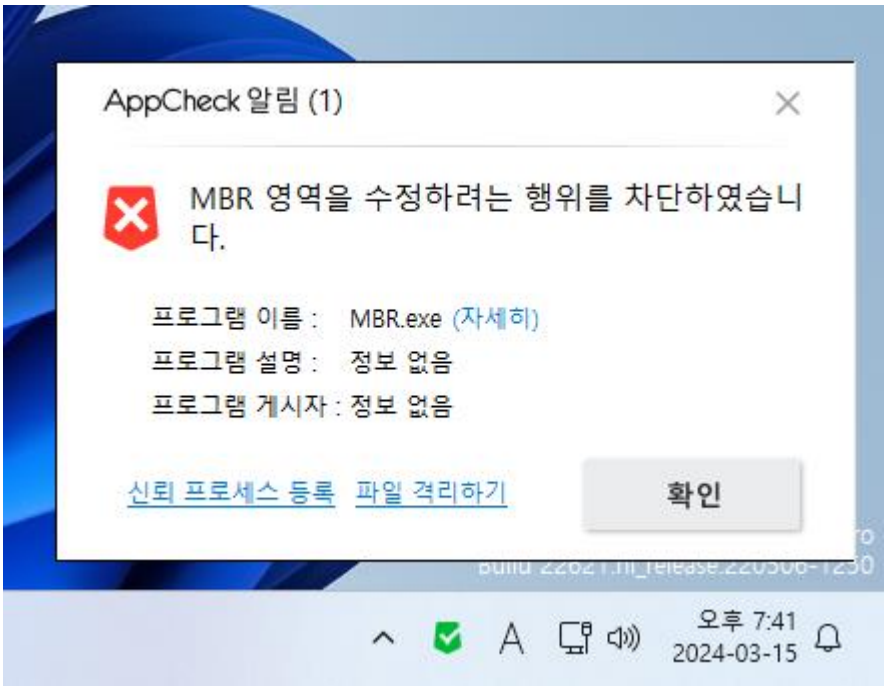
⊙ **알림 영역 아이콘 사용 :** 작업 표시줄의 시스템 트레이 아이콘에 AppCheck 안티랜섬웨어 아이콘 표시

"알림 영역 아이콘 사용" 옵션이 체크된 경우 AppCheck 안티랜섬웨어 아이콘(AppCheck.exe)이 종료되면 최대 2분 이내에 자동 재실행된다.

⊙ **프로그램 실행 차단시 알림창 실행 :** 랜섬웨어 행위 탐지(시스템 위협 차단 제외), MBR 보호, 취약점 가드 보호 기능을 통한 탐지 알림창 표시

⊙ **탐지시 의심 파일 전송하기 (익명으로 처리되며 분석 외 다른 용도로 사용되지 않습니다.) :** 랜섬웨어 행위 탐지(시스템 위협 차단 제외), 취약점 가드, MBR 보호 기능으로 탐지된 파일을 익명으로 체크멀(CheckMAL) 서버로 전송하기

⊙ **MBR 보호 :** Master Boot Record (MBR) 영역의 변조를 시도하는 파일 실행 차단 (탐지된 파일은 차단만 지원하며 자동 치료(제거)하지 않으며, 반복 재실행 시에는 랜섬웨어 행위 탐지로 삭제 처리된다.)



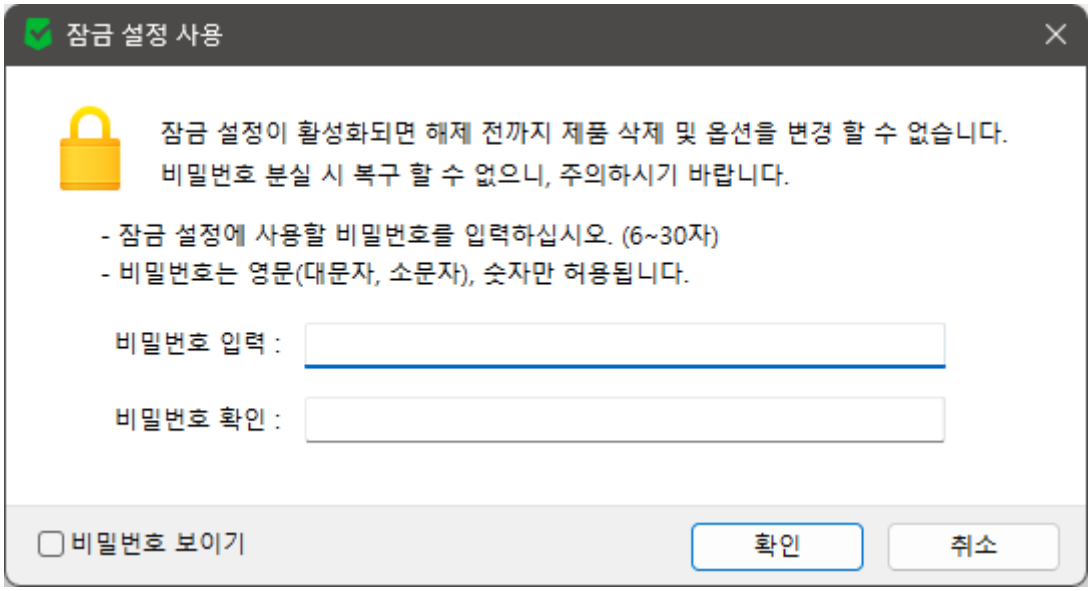
⊙ **자체 보호 사용 :** AppCheck 폴더(C:₩Program Files₩CheckMAL₩AppCheck, C:₩ProgramData₩CheckMAL₩AppCheck), 자동 백업 폴더(<AutoBackup(AppCheck)>), AppCheck 파일, AppCheck 레지스트리, AppCheck 안티랜섬웨어 서비스, AppCheckS.exe 서비스 프로세스, 일부 보안 제품 무력화 도구(※ 예시 : Process Explorer)로부터 AppCheck 종료 및 삭제로부터 보호

⊙ **잠금 설정 사용 :** 사용자가 입력한 비밀번호를 통해 AppCheck 옵션, 실시간 보호, AppCheck 제거 기능 변경 차단 (AppCheck Pro 전용)

단, CMS 중앙 관리를 통해 배포된 AppCheck Pro 버전은 Lock Mode 기능으로 대체되므로 옵션에서 "잠금 설정 사용" 메뉴가 표시되지 않는다.

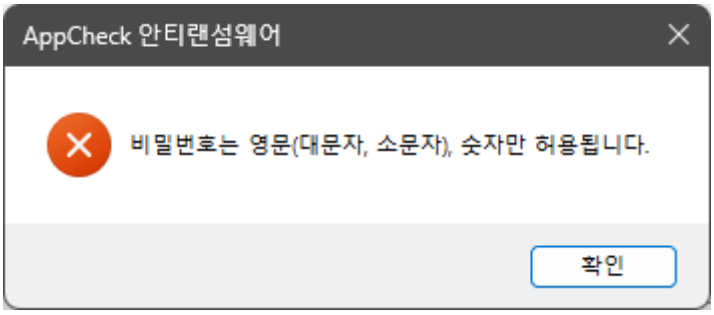
잠금 설정 사용을 위해서는 영문(대문자, 소문자) 또는 숫자로 구성된 6~30자리 길이의 비밀번호를 입력해야 하며, 비밀번호 분실 시 복구할 수 없다.

만약 잠금 설정에 사용된 비밀번호를 분실한 경우 체크멀 기술지원팀(support@checkmal.com)의 지원을 받아 AppCheck 제거를 통한 재설치 방식으로 해결할 수 있다.

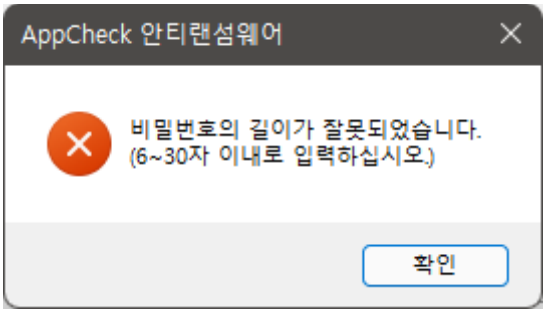


입력한 비밀번호를 확인하기 위해서는 "비밀번호 보이기" 박스에 체크하여 확인할 수 있다.

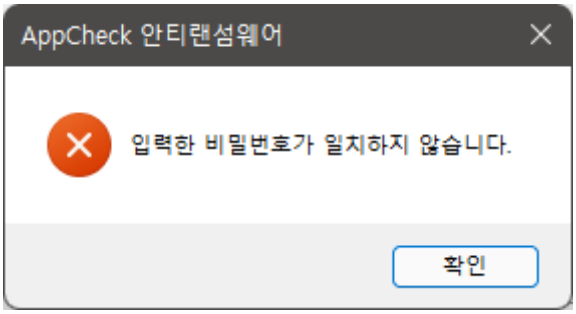
잠금 설정에서 허용하지 않는 문자를 입력 시 "비밀번호는 영문(대문자, 소문자), 숫자만 허용됩니다." 안내 메시지 창이 생성된다.



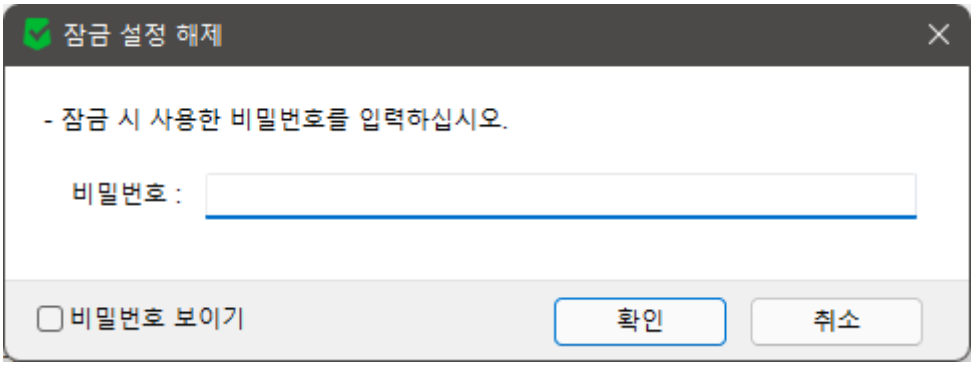
잠금 설정에 사용할 비밀번호 입력 시 6~30자리 길이로 지정하지 않을 경우 "비밀번호의 길이가 잘못되었습니다. (6~30자 이내로 입력하십시오.)" 안내 메시지 창이 생성된다.



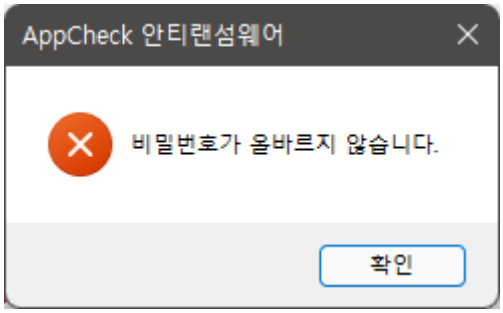
잠금 설정에 사용할 비밀번호 입력 후 비밀번호 확인란에 재입력 시 정보가 틀릴 경우 "입력한 비밀번호가 일치하지 않습니다." 안내 메시지 창이 생성된다.



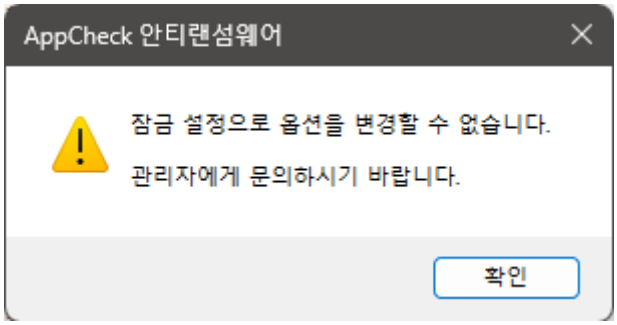
잠금 설정이 적용된 환경에서 AppCheck 옵션 메뉴 접근 시 잠금 설정 해제를 위한 비밀번호 입력창이 생성된다.



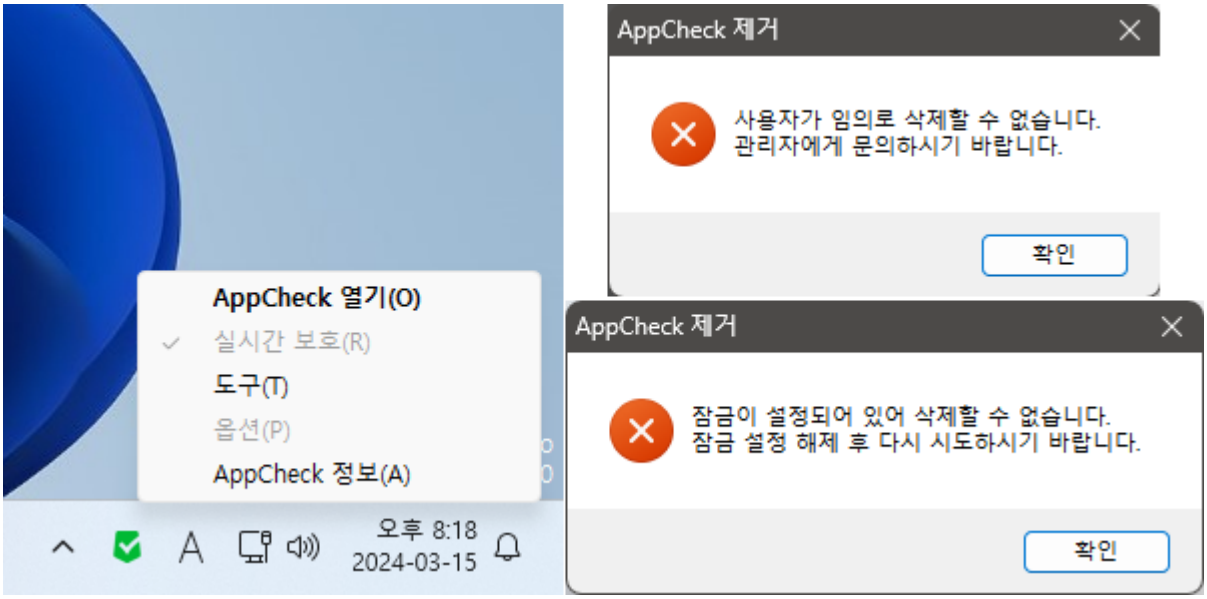
만약 입력한 비밀번호가 일치하지 않을 경우 "비밀번호가 올바르지 않습니다." 안내 메시지 창이 생성된다.



만약 CMS 중앙 관리 정책을 통해 Lock Mode가 적용된 환경에서는 AppCheck 옵션 접근 시 "잠금 설정으로 옵션을 변경할 수 없습니다. 관리자에게 문의하시기 바랍니다." 알내 메시지 창이 생성된다.



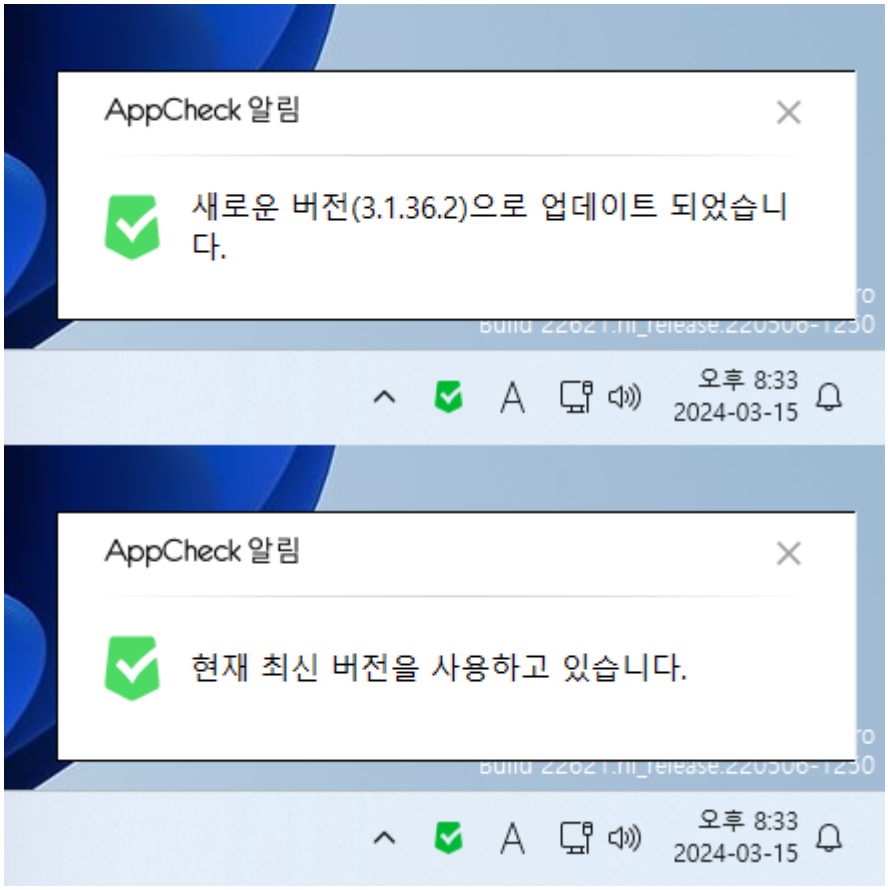
잠금 설정 사용 또는 CMS 중앙 관리 정책을 통한 Lock Mode가 적용된 AppCheck는 작업 표시줄의 시스템 트레이 아이콘 메뉴(실시간 보호, 옵션) 비활성화와 제어판에서 AppCheck 제거를 할 수 없다. (※ CMS 중앙 관리 정책에서는 "어플리케이션 제거 허용" 설정을 통해 AppCheck 제거 허용 여부를 결정할 수 있다.)



- **잠금 설정 사용 활성화 시 AppCheck 제거 메시지 :** 잠금이 설정되어 있어 삭제할 수 없습니다. 잠금 설정 해제 후 다시 시도하시기 바랍니다.
- **CMS 중앙 관리 정책에서 "어플리케이션 제거 허용" 미체크 시 AppCheck 제거 메시지 :** 사용자가 임의로 삭제할 수 없습니다. 관리자에게 문의하시기 바랍니다.

⊙ **자동 업데이트 사용 :** AppCheck Pro 버전은 3시간 주기로 체크멀 업데이트 서버와의 통신을 통해 상위 빌드 버전이 존재할 경우 자동 업데이트가 이루어진다. (AppCheck 무료 버전 : 6~12시간 주기)

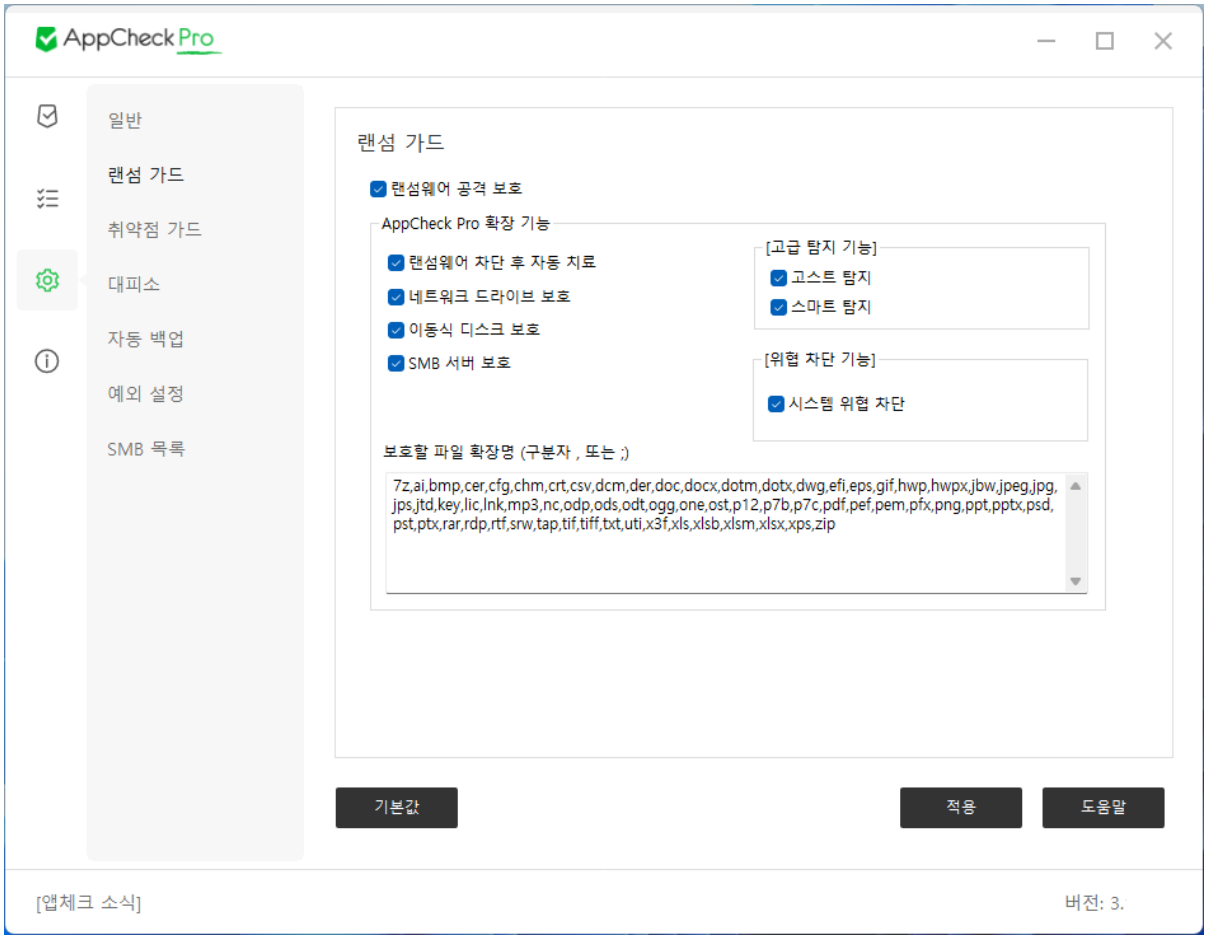
- **업데이트 에이전트로 사용 (AppCheck 무료 버전) :** P2P 방식으로 AppCheck 업데이트 동작 (선택 가능)



- **구버전에서 최신 버전으로 업데이트 시 AppCheck 업데이트 메시지 :** 새로운 버전(3.1.○.○)으로 업데이트 되었습니다.
- **최신 버전에서 업데이트 확인 시 메시지 :** 현재 최신 버전을 사용하고 있습니다.

⊙ **기본값 :** 일반 옵션 설정 초기화

[7-2] 랜섬 가드

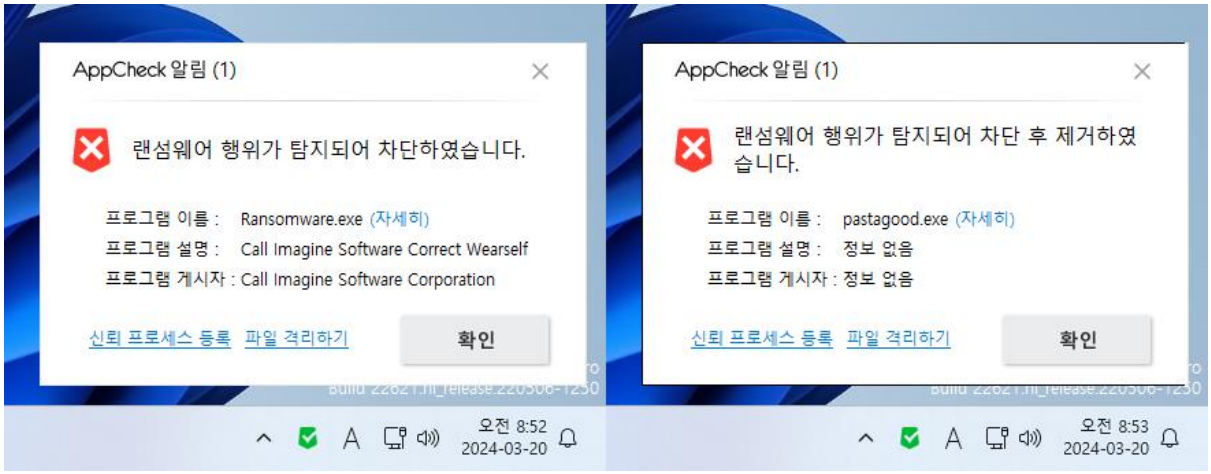


⊙ **랜섬웨어 공격 보호 :** 로컬/외장 디스크, USB 이동식 디스크, 네트워크 드라이브, SMB 서버 영역에 존재하는 보호할 파일 확장명에 포함된 파일들이 탐지 조건(기본값 : 10개 수준)에 따라 훼손될 경우 "랜섬웨어 행위 탐지", "랜섬웨어 행위 고급 탐지"를 통한 탐지 및 시스템 위협 차단 기능 전체를 제어할 수 있는 기능

랜섬웨어 공격 보호 기능이 정상적으로 동작하기 위해서는 "랜섬웨어 대피소 사용" 옵션이 반드시 활성화되어 있어야 한다.

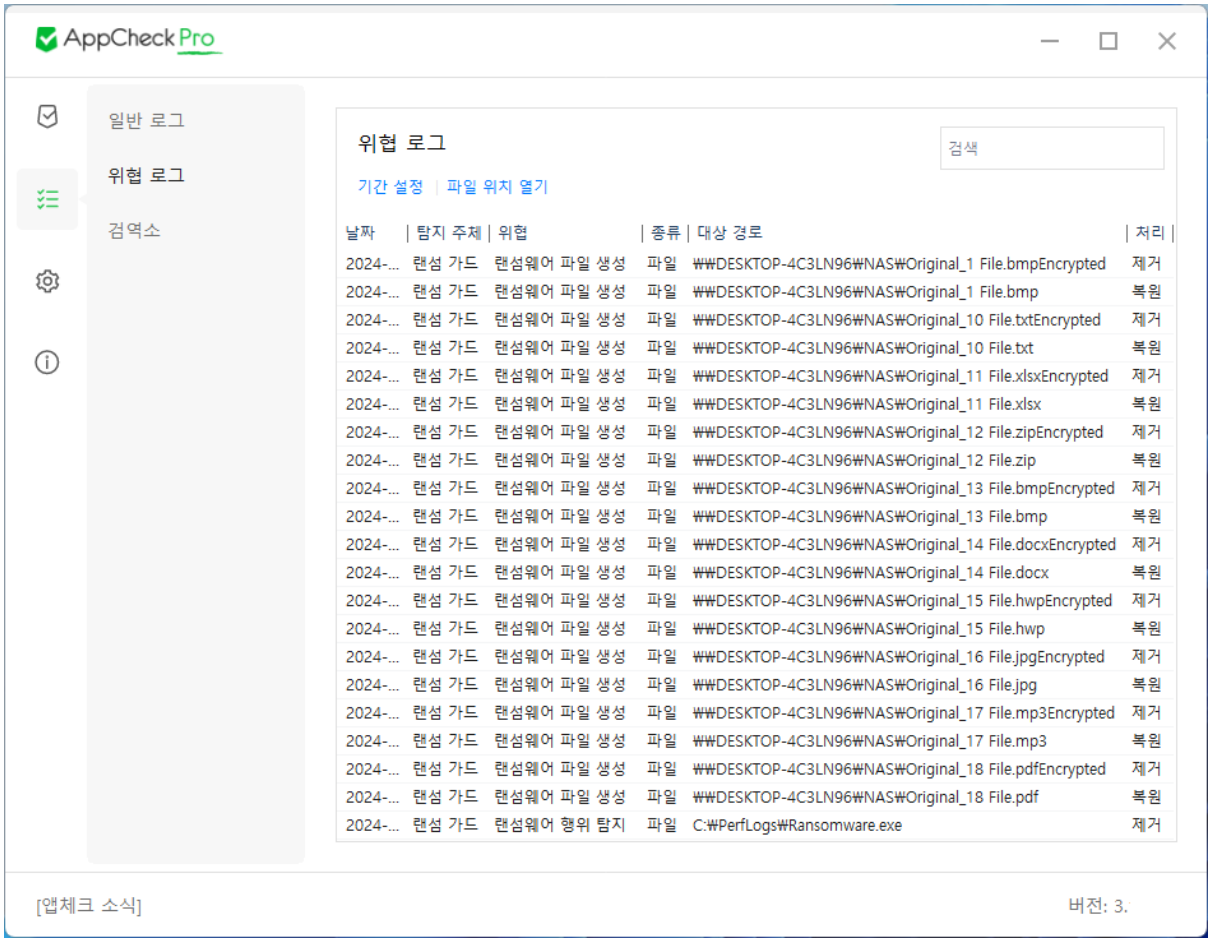
⊙ **AppCheck Pro 확장 기능 : 랜섬웨어 차단 후 자동 치료**

랜섬웨어 행위 탐지를 통해 탐지된 파일에 대한 자동 치료(제거)를 제공한다. 단, 차단된 파일 중 유효한 디지털 서명을 가진 파일 또는 시스템 폴더에 위치한 파일은 제거하지 않고 차단(종료)한다.



⊙ **AppCheck Pro 확장 기능 : 네트워크 드라이브 보호**

AppCheck가 설치된 PC에서 실행된 랜섬웨어(Ransomware)가 네트워크 드라이브로 연결된 다른 장치에 위치한 공유 폴더 내 파일 훼손 시 "랜섬웨어 행위 탐지"로 탐지 및 자동 복원한다.

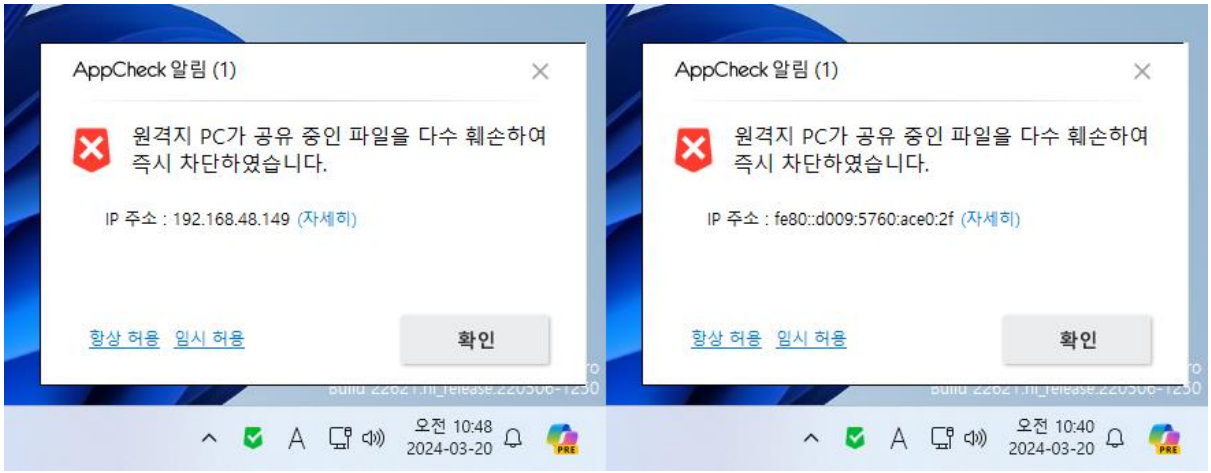


⊙ **AppCheck Pro 확장 기능 : 이동식 디스크 보호**

AppCheck가 설치된 PC에서 실행된 랜섬웨어(Ransomware)가 USB 포트로 연결된 이동식 디스크 내 파일을 훼손 시 "랜섬웨어 행위 탐지"로 탐지 및 자동 복원한다.

⊙ **AppCheck Pro 확장 기능 : SMB 서버 보호**

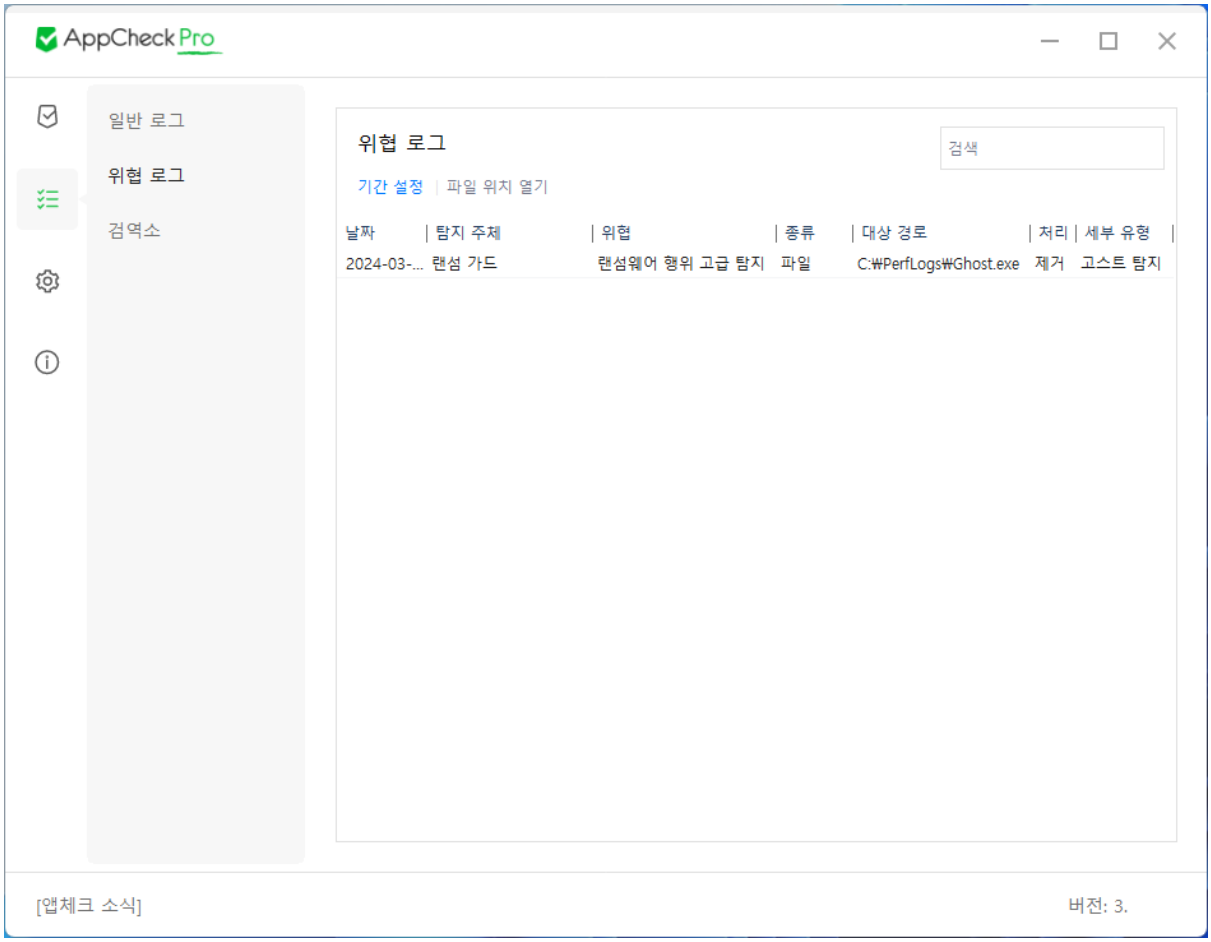
원격지 PC에서 실행된 랜섬웨어(Ransomware)가 네트워크 드라이브로 연결된 다른 장치의 공유 폴더(AppCheck 설치) 내 파일 훼손 시 원격지 IP 주소 임시 차단(1시간 후 자동 해제 또는 시스템 재부팅 시) 및 자동 복원한다.



⊙ **AppCheck Pro 확장 기능 : 고급 탐지 기능 - 고스트 탐지**

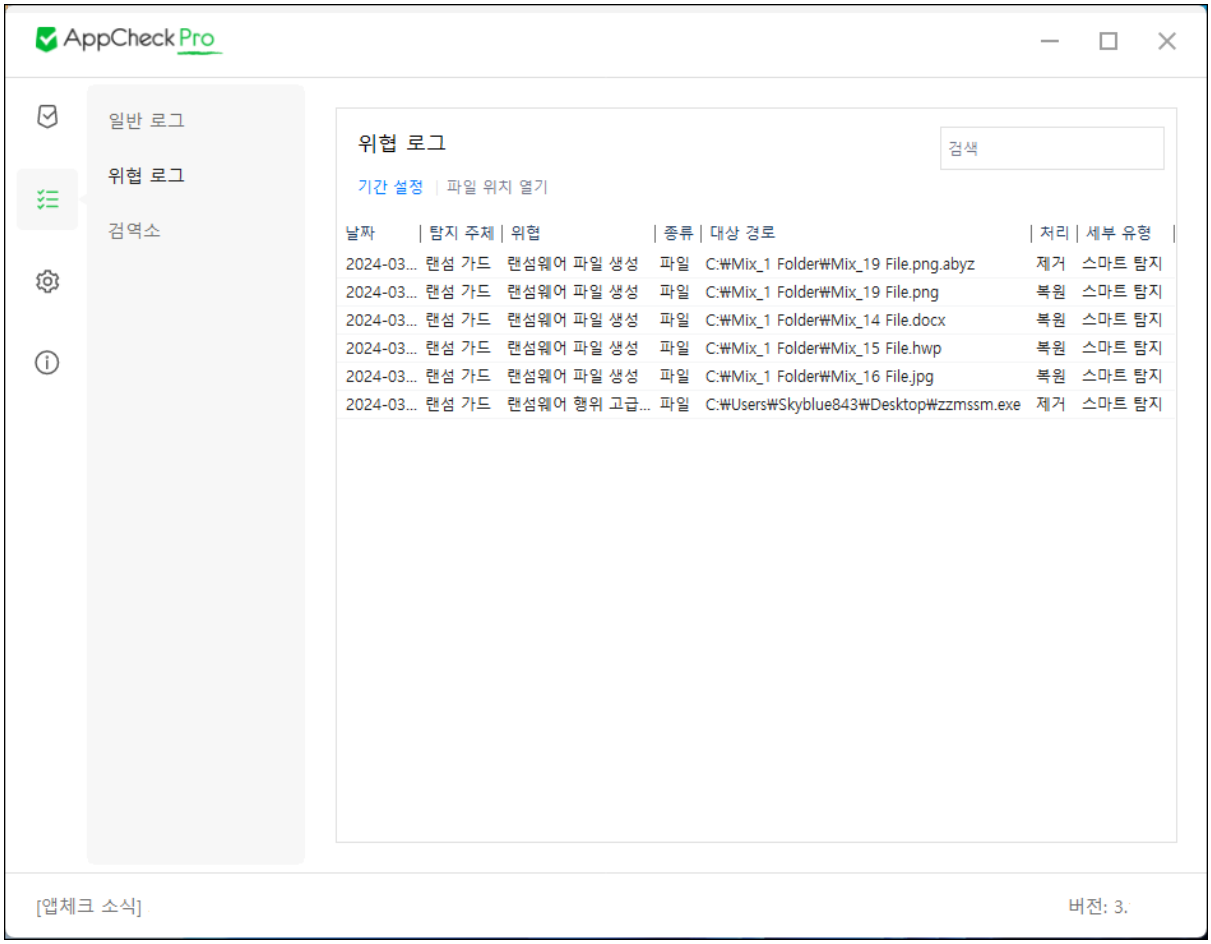
실행된 랜섬웨어 파일이 파일 목록을 열거할 경우 해당 프로세스의 메모리에 가상의 고스트(Ghost) 파일을 생성하여 해당 파일을 먼저 훼손하도록 유도하여 기존보다 빠른 탐지가 이루어지

도록 하는 "랜섬웨어 행위 고급 탐지" 방식이다.



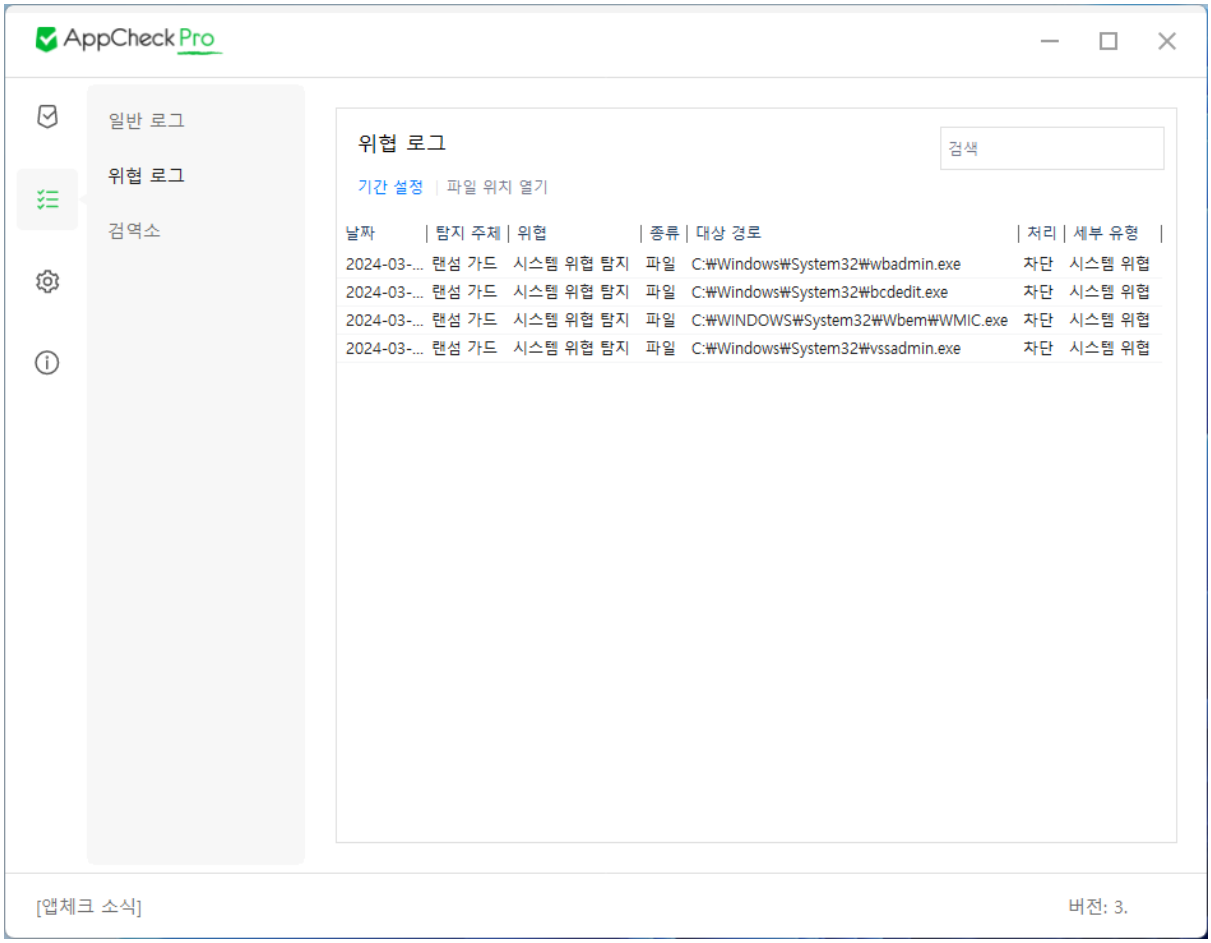
⊙ **AppCheck Pro 확장 기능 : 고급 탐지 기능 – 스마트 탐지**

실행된 랜섬웨어 프로세스(부모)가 다수의 자식 프로세스를 생성하여 순차 다중 방식으로 소수의 파일만 암호화한 후 종료 및 재실행을 반복하며 파일을 훼손할 경우 탐지할 수 있는 "랜섬웨어 행위 고급 탐지" 방식이다.



⊙ AppCheck Pro 확장 기능 : 위협 차단 기능 – 시스템 위협 차단

랜섬웨어를 비롯한 악성 프로그램이 시스템 복원 무력화, 안전 모드 부팅 명령어 등을 실행할 경우 사전 차단하여 시스템을 보호하는 탐지 방식이다.

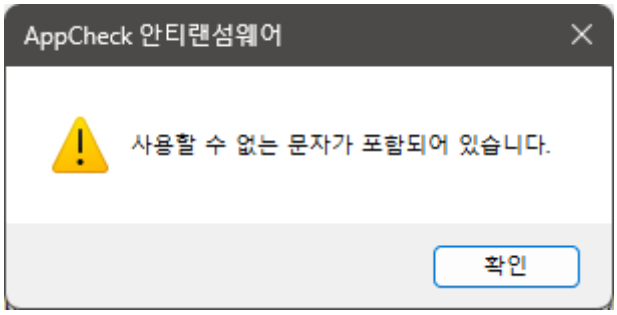


시스템 위협 차단 시 AppCheck 탐지 알림창은 생성하지 않으며, 위협 로그에만 시스템 위협 내역을 기록한다.

⊙ AppCheck Pro 확장 기능 : 보호할 파일 확장명 (구분자 , 또는 ;)

랜섬웨어에 의한 파일 훼손 행위로부터 보호되는 기본 파일 확장명은 총 65종 (7z,ai,bmp,cer,cfg,chm,crt,csv,dcm,der,doc,docx,dotm,dotx,dwg,efi,eps,gif,hwp,hwpx,jbw,jpeg,jpg,jps,jtd,key,lic,lnk,mp3,nc,odp,ods,odt,ogg,one,ost,p12,p7b,p7c,pdf,pef,pem,pfx,png,ppt,pptx,psd,pst,ptx,rar,rdp,rtf,srw,tap,tif,tiff,txt,uti,x3f,xls,xlsb,xlsm,xlsx,xps,zip)이며, 사용자에 의한 추가적인 파일 확장명 등록은 AppCheck Pro 정품 버전에서만 가능하다.

만약 보호할 파일 확장명에 추가한 문자 중 허용되지 않은 문자(※ 예시 : *)가 포함될 경우 "사용할 수 없는 문자가 포함되어 있습니다." 알림 메시지 창을 생성하여 적용되지 않도록 한다.

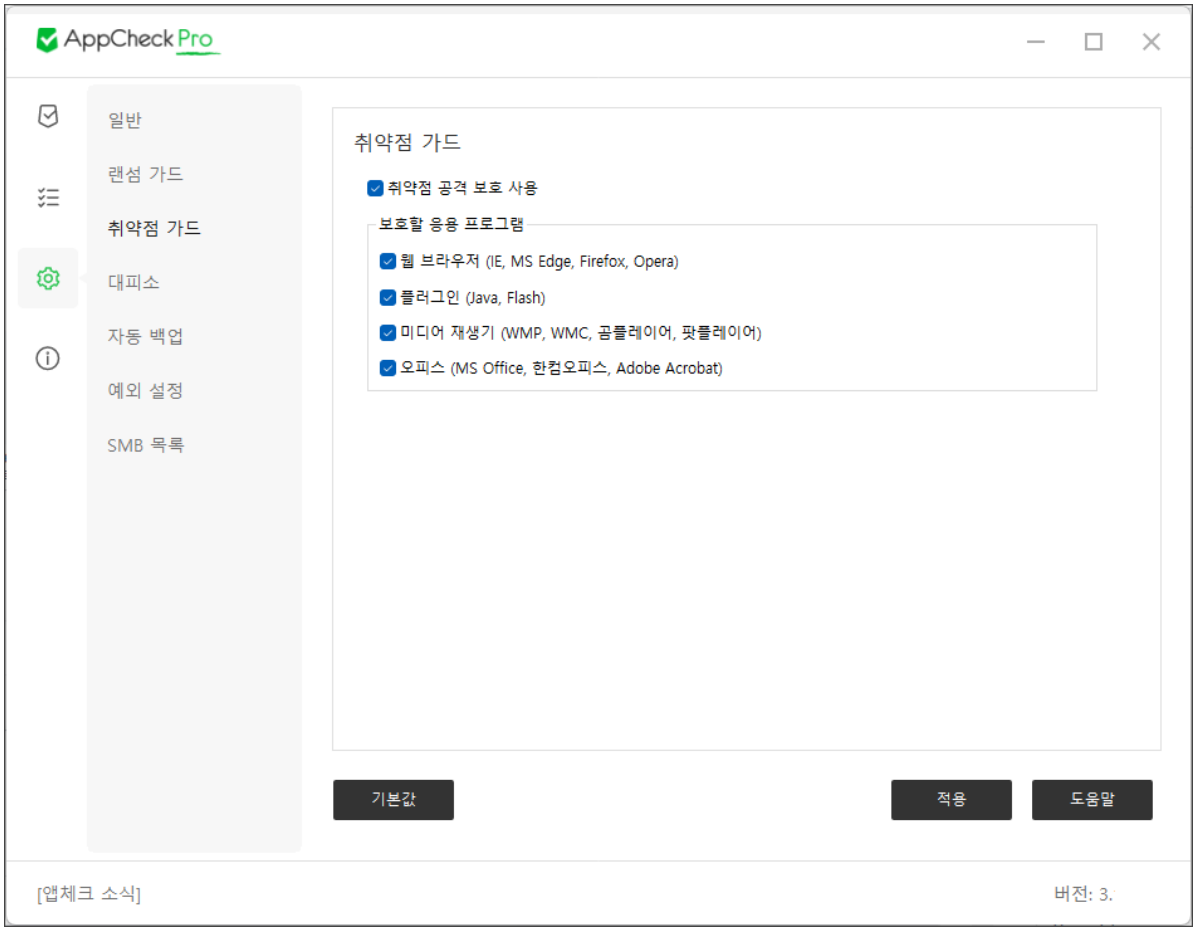


⊙ **기본값 :** 랜섬 가드 옵션 설정 초기화

[7-3] 취약점 가드

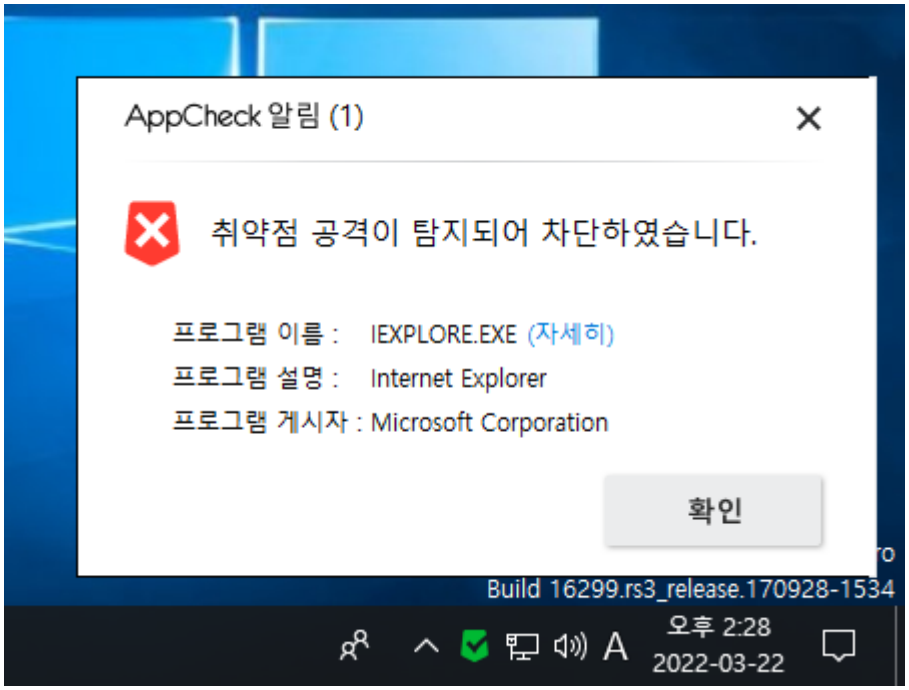
취약점 가드는 보호할 응용 프로그램의 취약점(Exploit) 코드 실행이 이루어질 경우 취약점 공격 탐지를 통해 사전 차단하여 악성코드 자동 감염을 예방하는 보호 기능이다.

보호할 응용 프로그램 중 오피스(Office) 프로그램은 AppCheck Pro 정품 버전에서만 활성화할 수 있다.



웹 브라우저	Internet Explorer, Microsoft Edge, Firefox, Opera
플러그인	Java, Adobe Flash
미디어 재생기	Windows Media Player, Windows Media Center, 곰플레이어(GomPlayer), 팟플레이어(PotPlayer)
오피스	Microsoft Office, 한컴오피스, Adobe Acrobat

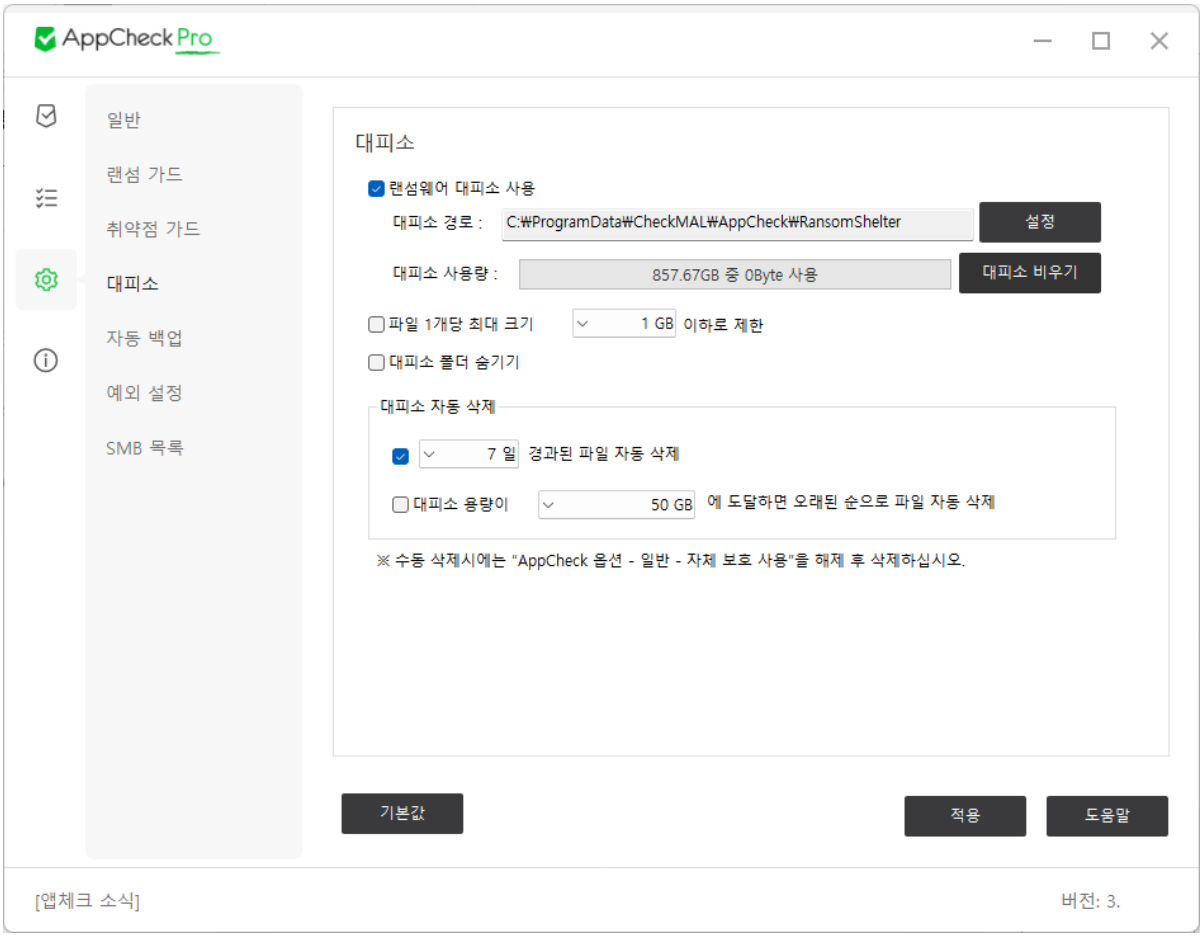
취약점 공격 탐지가 발생한 시스템은 차단된 응용 프로그램을 확인하여 Windows 업데이트 기능을 통한 최신 보안 패치 적용 및 각 응용 프로그램의 최신 버전을 확인하여 구버전인 경우 최신 버전으로 업데이트하여 취약점 문제를 수정해야 한다.



- **프로그램 이름 :** 취약점 공격을 탐지하여 차단된 보호할 응용 프로그램의 실행 파일명
- **프로그램 이름 (자세히) :** "도구 – 위협 로그" 메뉴로 자동 연결
- **프로그램 설명 :** 취약점 공격을 탐지하여 차단된 파일 속성에 표시된 파일 설명
- **프로그램 게시자 :** 취약점 공격을 탐지하여 차단된 파일의 디지털 서명 이름

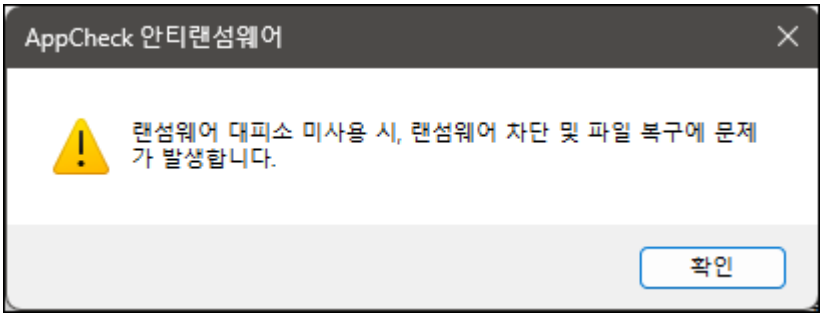
⊙ **기본값 :** 취약점 가드 옵션 설정 초기화

[7-4] 대피소

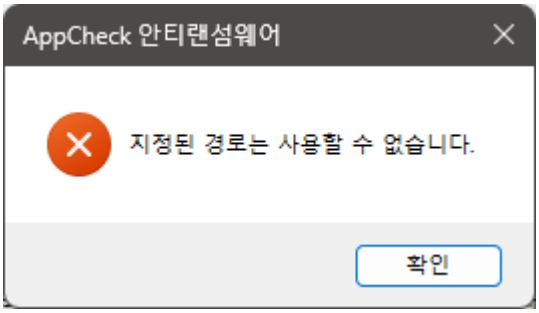


⊙ **랜섬웨어 대피소 사용 :** 보호할 파일 확장명에 포함된 파일이 특정 조건에 따라 변경, 삭제 등 의심스러운 파일 훼손이 발생할 경우 실시간으로 랜섬웨어 대피소 폴더에 복사본(Copy)을 임시 백업하며, 랜섬웨어 행위 탐지 시 대피소에 임시 백업된 파일을 이용하여 원래 위치로 자동 복원해주는 기능이다.

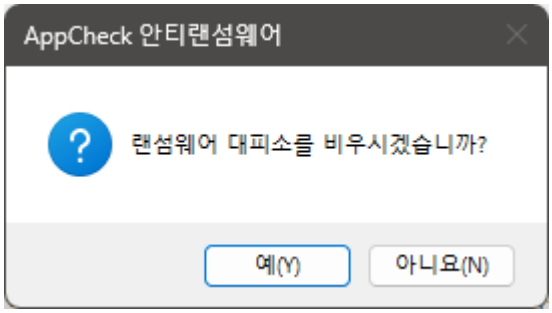
랜섬웨어 대피소 기능을 사용하지 않을 경우 "랜섬웨어 대피소 미사용 시 랜섬웨어 차단 및 파일 복구에 문제가 발생합니다." 알림 메시지 창이 생성되며, 랜섬웨어 미탐지 또는 랜섬웨어 탐지 후 탐지 이전에 일부 훼손된 보호 대상 파일에 대한 자동 복원을 할 수 없다.



- **대피소 경로 :** 대피소 기본 위치는 "C:₩ProgramData₩CheckMAL₩AppCheck₩RansomShelter" 폴더이며, "설정" 버튼을 클릭하여 원하는 다른 폴더로 변경 가능하다. 단, 특정 위치로 대피소 경로를 지정할 경우 "지정된 경로는 사용할 수 없습니다." 알림 메시지 창이 생성되므로 다른 폴더로 지정해야 한다. 참고로 네트워크 드라이브를 대피소 경로로 지정하면 안된다.



- **대피소 사용량 :** 대피소 경로로 지정된 디스크의 전체 용량 중 대피소 내 저장된 파일 용량 표시
- **대피소 비우기 :** 대피소 폴더 및 내부 파일을 일괄 삭제하며, 삭제된 폴더 및 내부 파일은 휴지통으로 이동되지 않고 완전 삭제된다. 사용자가 "대피소 비우기" 버튼 클릭 시 "랜섬웨어 대피소를 비우시겠습니까?" 알림 메시지 창이 생성된다.



만약 랜섬웨어 대피소 폴더 내 파일을 수동 삭제 시에는 "AppCheck 옵션 – 일반 – 자체 보호 사용" 박스를 체크 해제 후 삭제한다.

- **파일 1개당 최대 크기 :** 대피소에 임시 백업되는 파일 1개 최대 크기(100MB, 200MB, 500MB, 1GB, 2GB, 5GB) 이하로 제한
- **대피소 폴더 숨기기 :** 대피소 폴더 속성을 숨김(H) 처리
- **대피소 자동 삭제 – ○일 경과된 파일 자동 삭제 :** 대피소 폴더에 임시 백업된 파일을 "10분, 20분, 30분, 1시간, 3시간, 6시간, 12시간, 1일, 2일, 3일, 4일, 5일, 6일, 7일" 경과 시 자동 삭제 (기본값 : 7일)

만약 대피소 자동 삭제 시간을 너무 짧게 설정할 경우 수동 복구가 필요한 경우 임시 백업된 파일이 삭제되어 복구할 수 없으므로 기간 설정에 주의해야 한다.

- **대피소 자동 삭제 – 대피소 용량이 ○○에 도달하면 오래된 순으로 파일 자동 삭제 :** 대피소 폴더에 임시 백업된 전체 파일 용량이 "5GB, 10GB, 20GB, 50GB, 100GB, 디스크의 10%, 디스크의 20%, 디스크의 30%, 디스크의 40%, 디스크의 50%"에 도달하면 오래된 파일순으로 자동 삭제 (기본값 : 50GB)

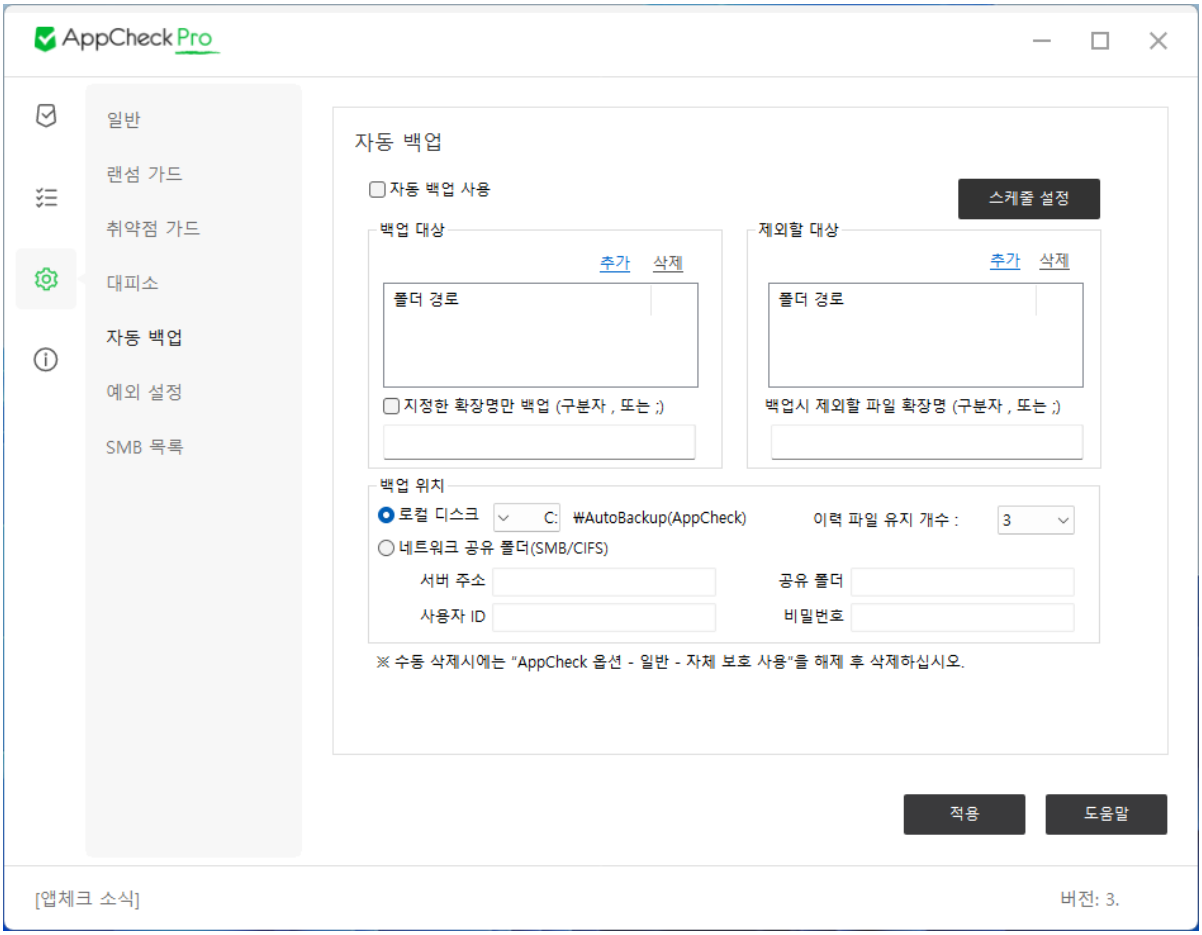
⊙ **기본값 :** 대피소 옵션 설정 초기화

[7-5] 자동 백업

자동 백업은 백업 대상 폴더를 추가하여 폴더 내의 모든 파일을 자동 백업 폴더 <AutoBackup(AppCheck)>에 파일 히스토리(History) 기반으로 스케줄 설정에 따라 백업한다.

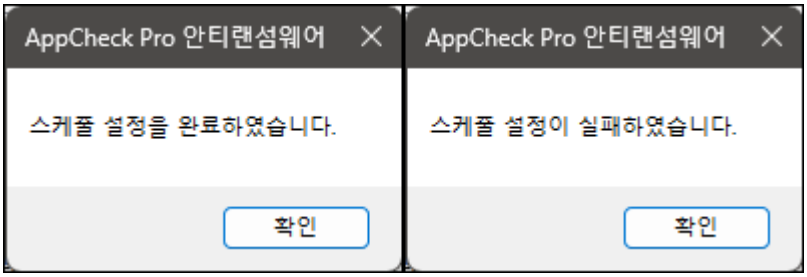
자동 백업 폴더에 저장된 파일은 자체 보호 기능을 통해 랜섬웨어에 의해 훼손되지 않도록 보호 받는다.

자동 백업된 파일을 안전하게 보호하기 위해서는 백업 대상 폴더에 추가된 디스크가 아닌 다른 저장 장치에 백업이 이루어지도록 설정해야 한다.

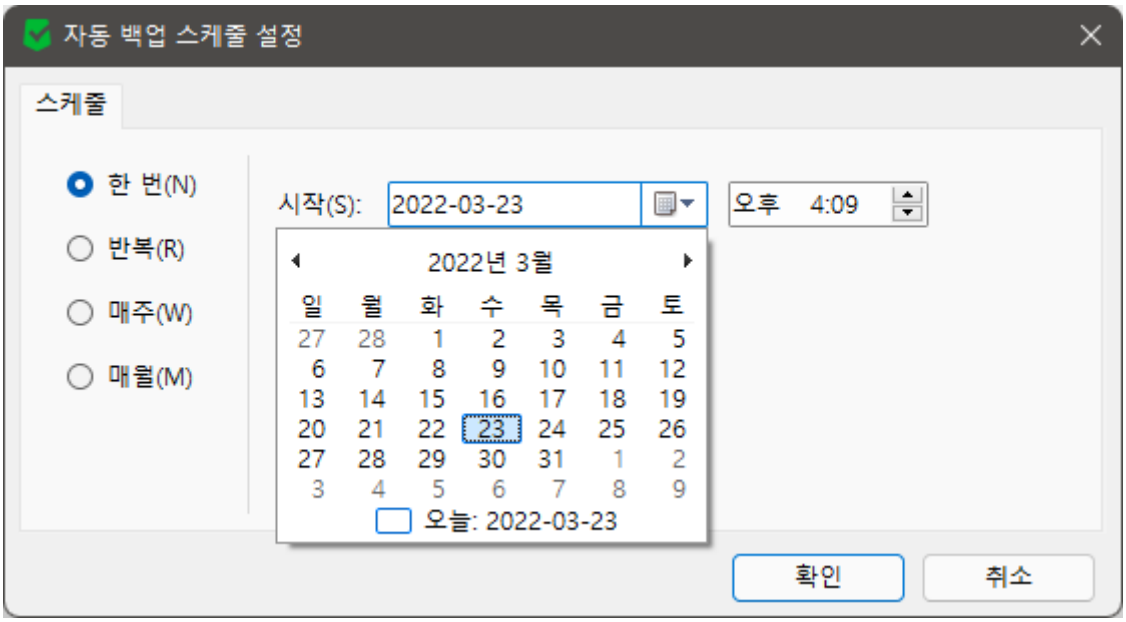


⊙ **스케줄 설정 :** 한 번, 반복, 매주, 매월 단위로 자동 백업

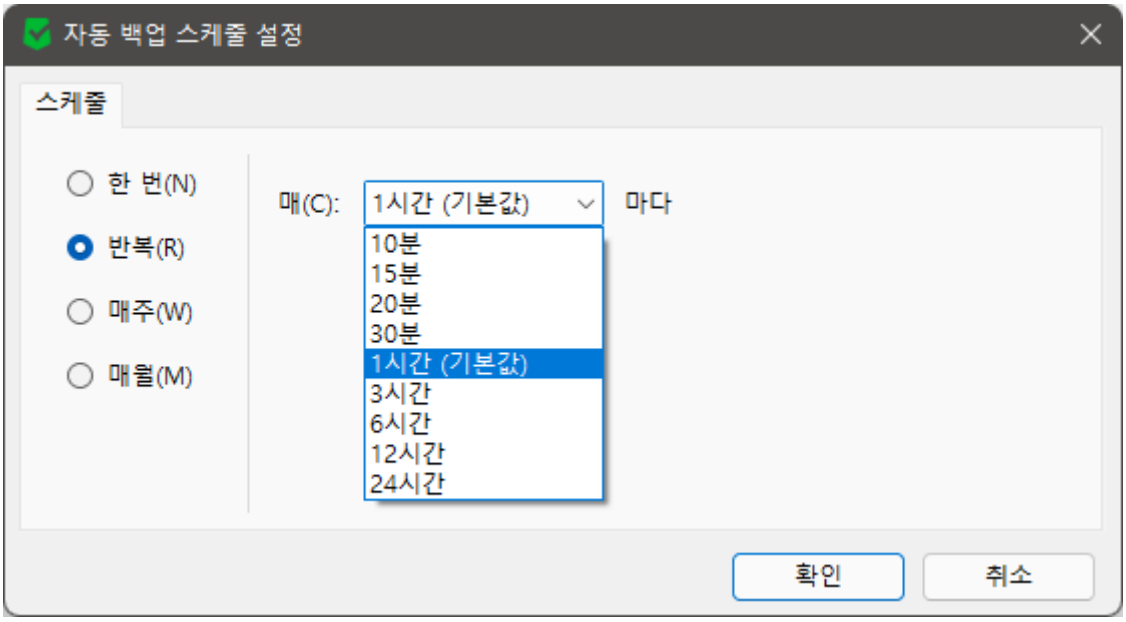
스케줄 설정을 변경한 후 "확인" 버튼 클릭 시 "스케줄 설정을 완료하였습니다." 안내 메시지 창이 생성되며, 유효하지 않은 스케줄 설정을 한 후 "확인" 버튼 클릭 시 "스케줄 설정이 실패하였습니다." 알림 메시지 창이 생성된다.



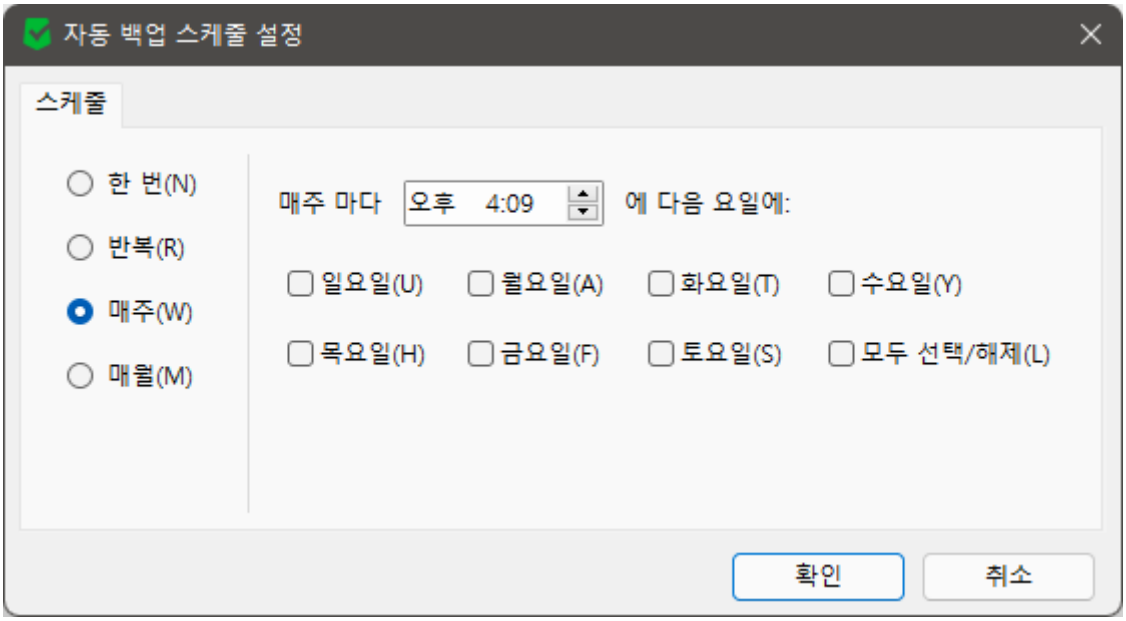
- **한 번 :** 지정한 특정일의 특정 시간에 1회 자동 백업한다.



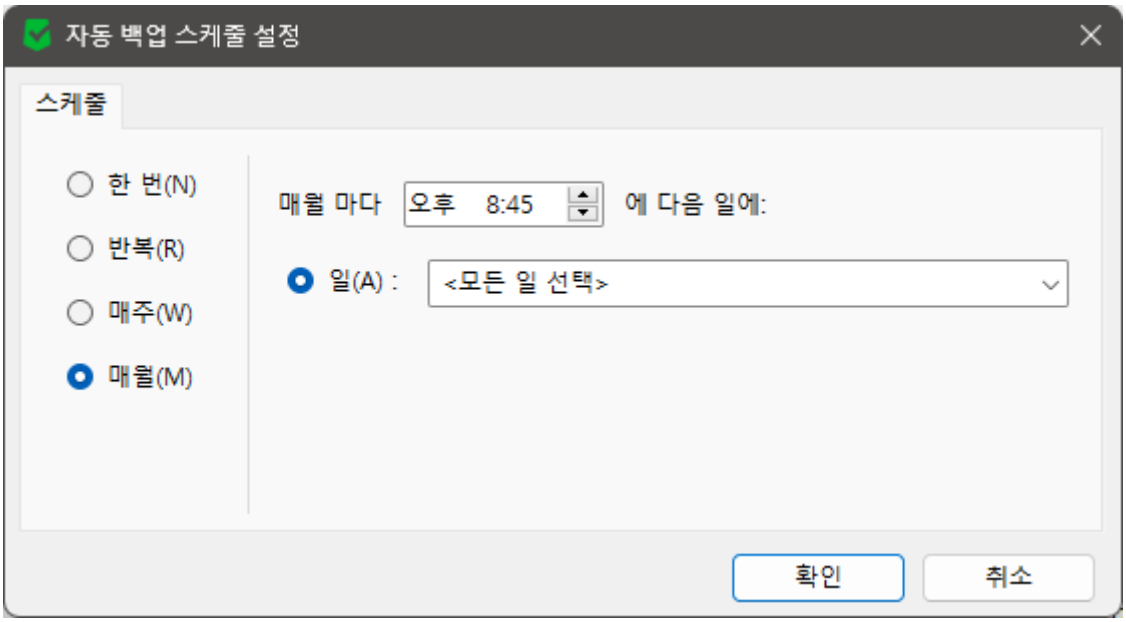
- **반복 :** 10분, 15분, 20분, 30분, 1시간(기본값), 3시간, 6시간, 12시간, 24시간 단위로 자동 백업하며, Windows 부팅 후 1분 경과 시 자동 백업이 진행된다.



- **매주 :** 지정한 특정 요일의 특정 시간에 자동 백업한다.

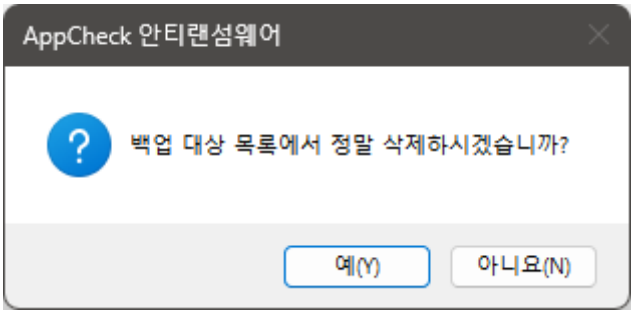


- **매월 :** 매월 지정한 특정일의 특정 시간에 자동 백업한다.



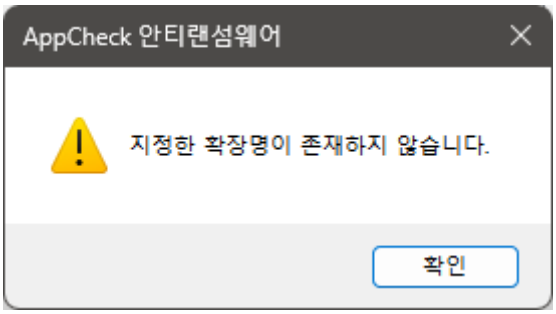
⊙ **백업 대상 :** 백업을 원하는 폴더(하위 폴더 포함) 추가 및 삭제

백업 대상에 추가된 폴더 삭제 시 "백업 대상 목록에서 정말 삭제하시겠습니까?" 알림 메시지 창이 생성된다.



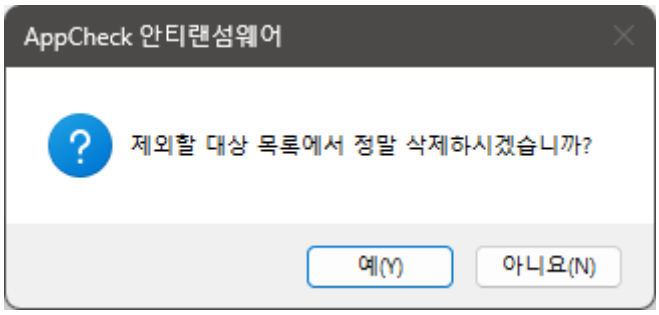
⊙ **지정한 확장명만 백업 (구분자 , 또는 ;) :** 백업 대상 폴더 내에 존재하는 파일 중 사용자가 지정한 파일 확장명만 백업 (※ 예시 : docx,jpg,pdf)

지정한 확장명 추가없이 "지정한 확장명만 백업" 박스에 체크 후 "적용" 버튼 클릭 시 "지정한 확장명이 존재하지 않습니다." 알림 메시지 창이 생성되어 옵션 저장에 실패한다.



⊙ **제외할 대상 :** 백업 대상 폴더에 추가된 하위 폴더 중 자동 백업 시 제외를 원하는 폴더 추가 및 삭제

제외할 대상에 추가된 폴더 삭제 시 "제외할 대상 목록에서 정말 삭제하시겠습니까?" 알림 메시지 창이 생성된다.



⊙ **백업 시 제외할 파일 확장명 (구분자 , 또는 ;) :** 백업 대상 폴더 내에 존재하는 파일 중 사용자가 지정한 파일 확장명은 백업 시 제외 처리 (※ 예시 : odp#,ods#,odt#)

⊙ **백업 위치 :** 로컬 디스크 또는 네트워크 공유 폴더(SMB/CIFS) 중 선택

⊙ **로컬 디스크 :** PC와 물리적으로 연결된 디스크 중 여유 공간이 가장 많은 디스크가 기본적으

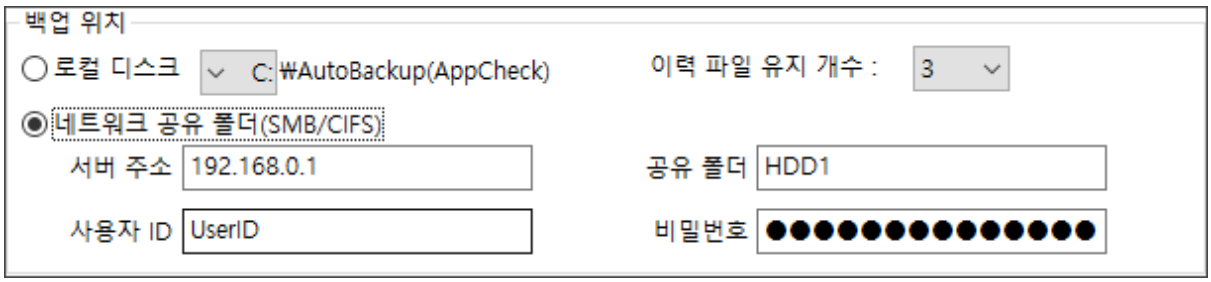
로 자동 선택되며, 사용자 선택에 따라 자동 백업 폴더<AutoBackup(AppCheck)>가 저장될 디스크를 지정할 수 있다.

⊙ **이력 파일 유지 개수 :** 백업 대상 폴더로 추가되어 백업된 원본 파일이 수정될 경우 기존의 백업 파일은 이력 파일(.history)로 변경되며, 이력 파일 수는 0~10개로 사용자가 지정할 수 있다. (기본값 : 3개)

- 이력 파일 생성 예시 : AppCheck.docx.20240320210222.history

이력 파일 유지 개수를 초과할 경우 가장 오래된 이력 파일부터 자동 삭제하여 이력 파일 유지 개수를 맞춘다.

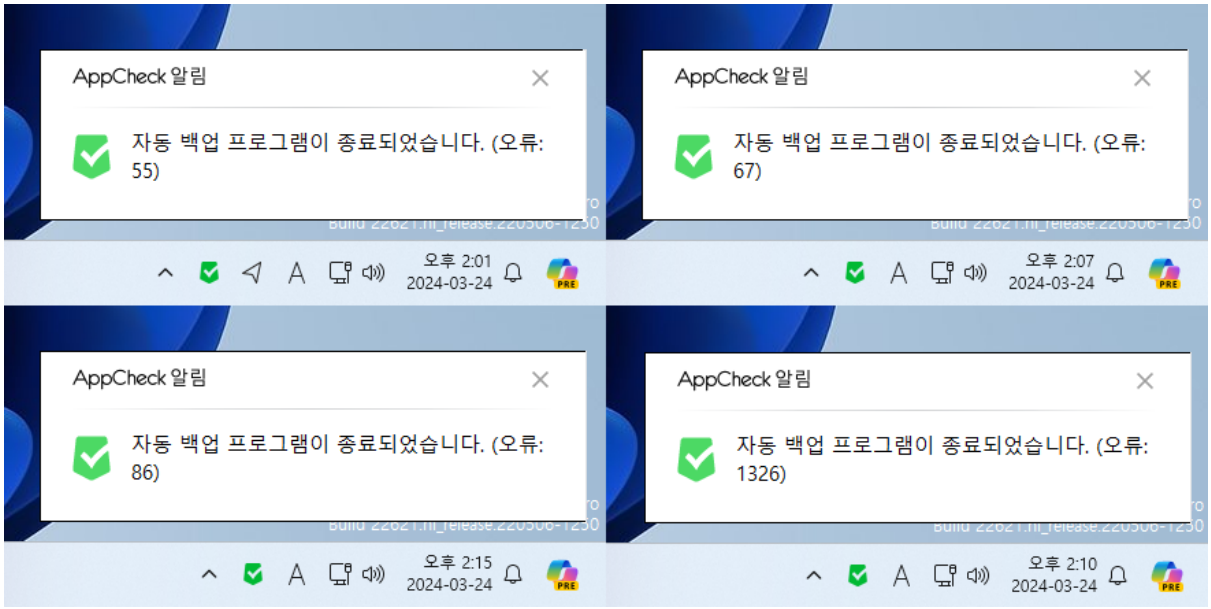
⊙ **네트워크 공유 폴더(SMB/CIFS) :** SMB 방식으로 연결 가능한 서버 주소(IP 주소 / 도메인 주소 또는 원격지 장치 이름), 공유 폴더(공유 설정이 이루어진 원격지 최상위 폴더 이름부터 입력), 사용자 ID, 비밀번호를 입력한다.



- 네트워크 공유 폴더 설정값에 따른 자동 백업 폴더 생성 예시
  - HDD1 : ₩₩192.168.0.1₩hdd1₩AutoBackup(AppCheck)
  - HDD1₩Backup : ₩₩192.168.0.1₩hdd1₩Backup₩AutoBackup(AppCheck)

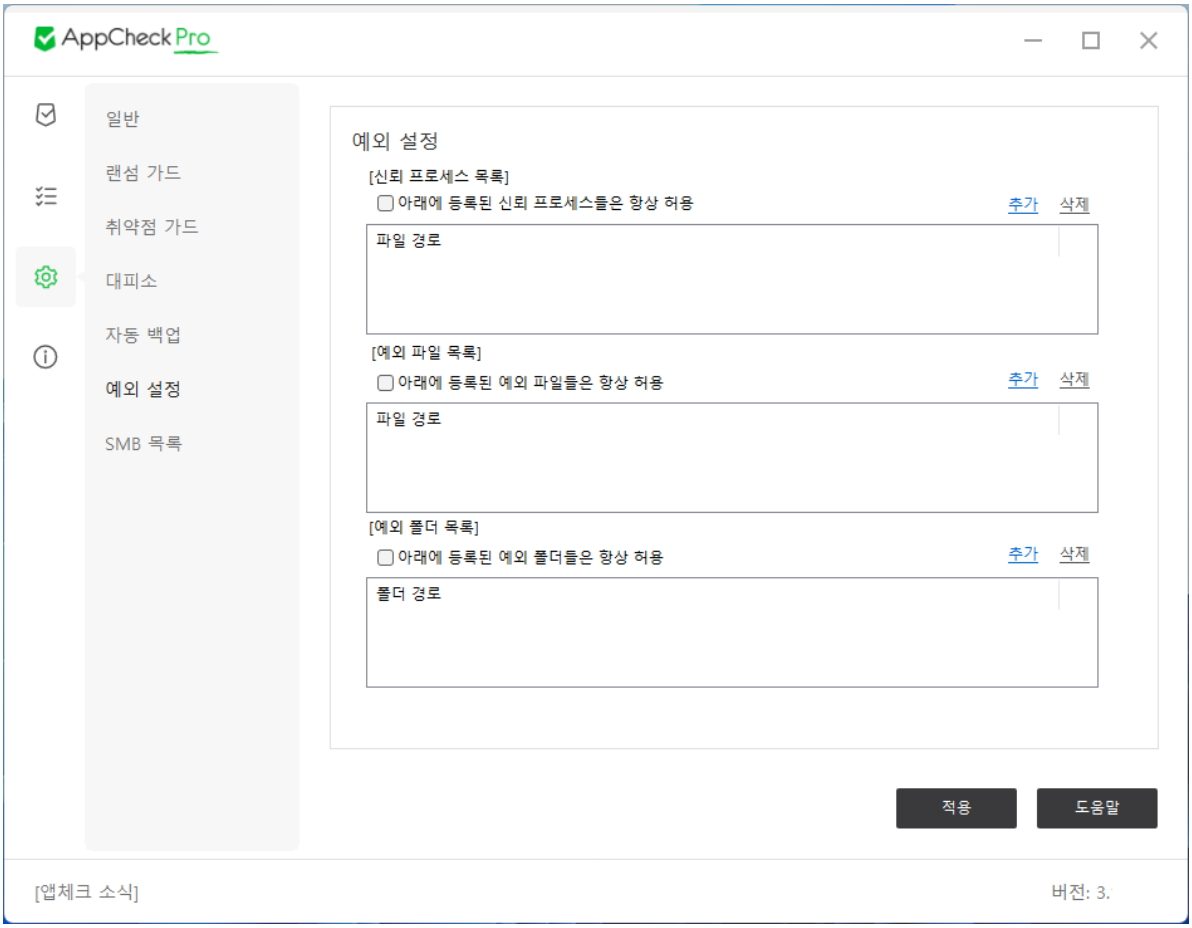
네트워크 공유 폴더의 서버 주소 입력 시 IPv4 주소로 입력하지 않을 경우 자동 백업 폴더 내 파일을 보호받지 못할 수 있다.

자동 백업을 위한 네트워크 공유 폴더 설정값 중 일부 유효하지 않은 정보가 포함될 경우 자동 백업 시 "자동 백업 프로그램이 종료되었습니다. (오류: 55 / 67 / 86 / 1326)" 에러 알림창이 생성된다.



자동 백업 폴더<AutoBackup(AppCheck)> 및 내부 파일을 삭제하기 위해서는 "옵션 – 일반 – 자체 보호 사용" 설정을 체크 해제 후 폴더 및 파일을 수동 삭제할 수 있다.

[7-6] 예외 설정

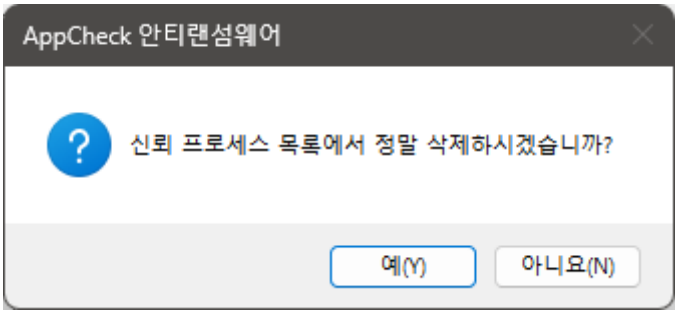


⊙ 신뢰 프로세스 목록

신뢰 프로세스 목록에 추가된 파일은 랜섬웨어 행위 탐지, 랜섬웨어 행위 고급 탐지(고스트 탐지, 스마트 탐지), MBR 차단이 발생하지 않도록 허용한다. 단, 특정 의심스러운 탐지 조건에 따라서는 신뢰 프로세스 목록에 추가된 파일에 대한 탐지가 이루어질 수 있다.

- **아래에 등록된 신뢰 프로세스들은 항상 허용 :** 신뢰 프로세스 목록에 추가된 파일은 탐지하지 않도록 허용한다.
- **신뢰 프로세스 목록 추가 (예시) :** C:₩Program Files (x86)₩VMware₩VMware Workstation₩vmware.exe

신뢰 프로세스 목록에 추가된 항목 선택 후 삭제 시 "신뢰 프로세스 목록에서 정말 삭제하시겠습니까?" 알림 메시지 창이 생성된다.



기본적으로 신뢰 프로세스 목록에 추가된 파일에 의해 훼손되는 파일들은 랜섬웨어 대피소 폴더에 백업 처리가 이루어지지 않는다.

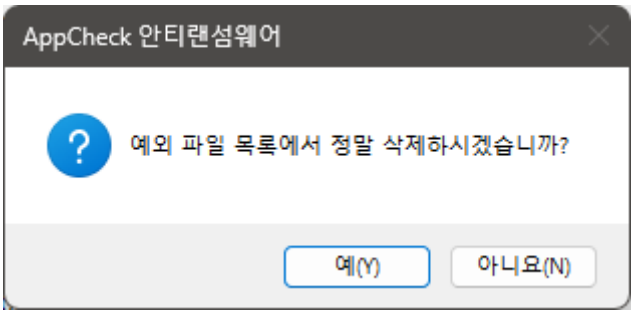
신뢰 프로세스 목록 추가 시 랜섬웨어에 의해 악용 가능성이 상대적으로 높은 Windows 시스템 파일(Explorer.exe, svchost.exe 등)을 등록할 경우 탐지되지 않을 수 있으므로 일부 사용자만 제한적으로 추가하도록 한다.

⊙ 예외 파일 목록

예외 파일 목록은 AppCheck 보호할 파일 확장명에 포함된 파일 중 보호를 원하지 않는 경우 예외 파일 목록에 추가한다. 단, 네트워크 드라이브 영역에 대해서는 지원하지 않는다.

- **아래에 등록된 예외 파일들은 항상 허용 :** 예외 파일 목록에 추가된 파일은 AppCheck 보호 대상에서 제외 처리되어 대피소 백업 및 복원을 지원하지 않는다.
- **예외 파일 목록 추가 (예시) :** D:₩자료실₩문서₩개인 문서₩목록.pdf

예외 파일 목록에 추가된 항목 선택 후 삭제 시 "예외 파일 목록에서 정말 삭제하시겠습니까?" 알림 메시지 창이 생성된다.



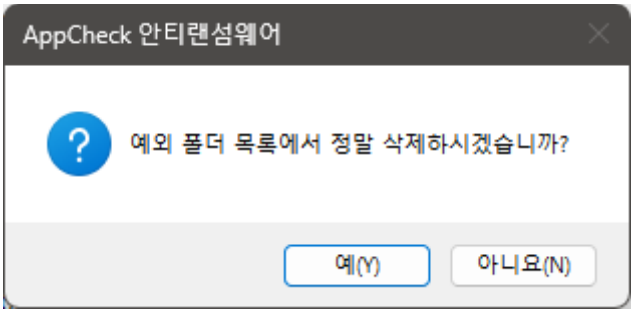
⊙ 예외 폴더 목록

예외 폴더 목록에 추가된 폴더 및 하위 폴더는 AppCheck 보호를 원하지 않는 경우 지원한다. 단, 네트워크 드라이브 영역에 대해서는 지원하지 않는다.

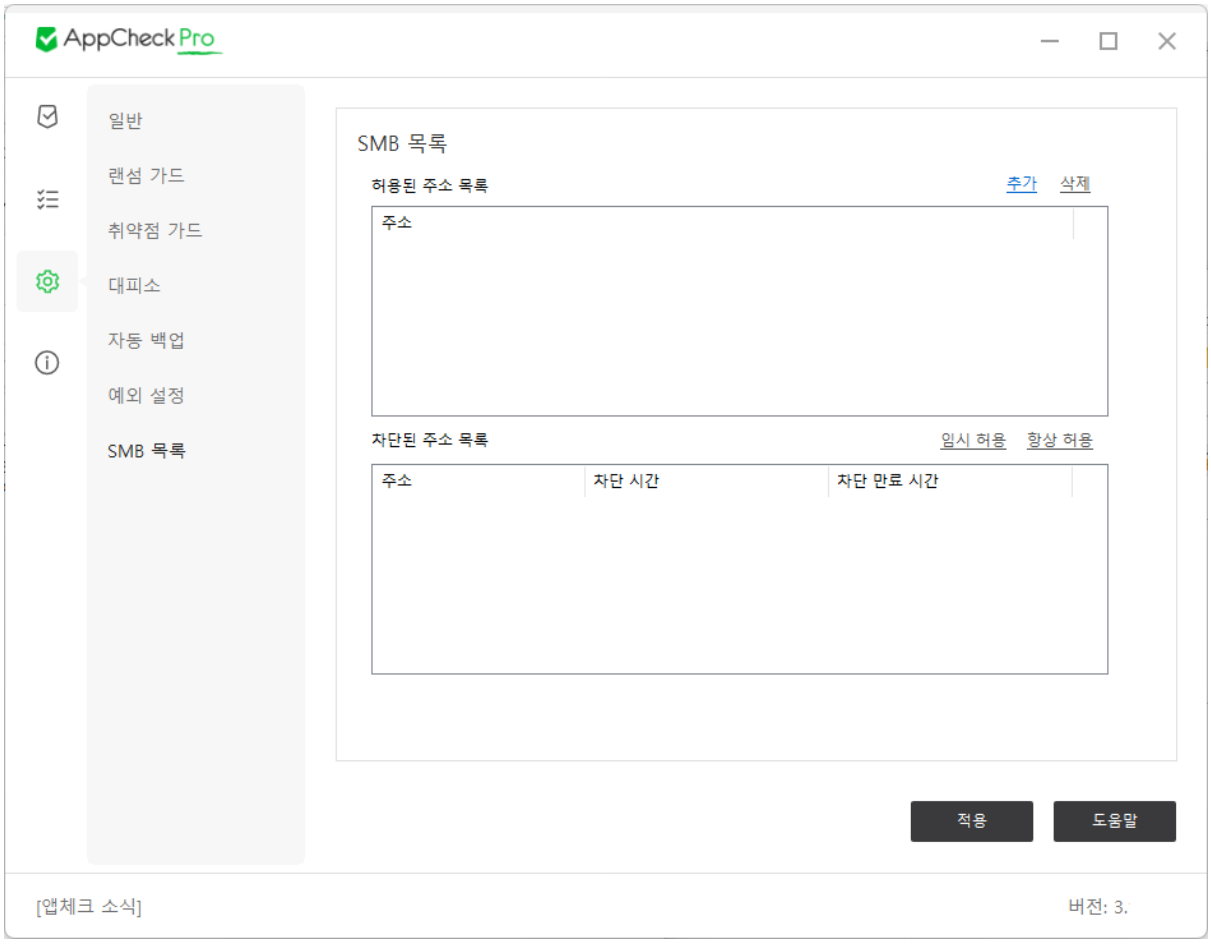
- **아래에 등록된 예외 폴더들은 항상 허용 :** 예외 폴더 목록에 추가된 폴더 내 모든 파일은 AppCheck 보호 대상에서 제외 처리되어 대피소 백업 및 복원을 지원하지 않는다.

- **예외 폴더 목록 추가 (예시) :** C:₩Program Files₩7-Zip₩Lang

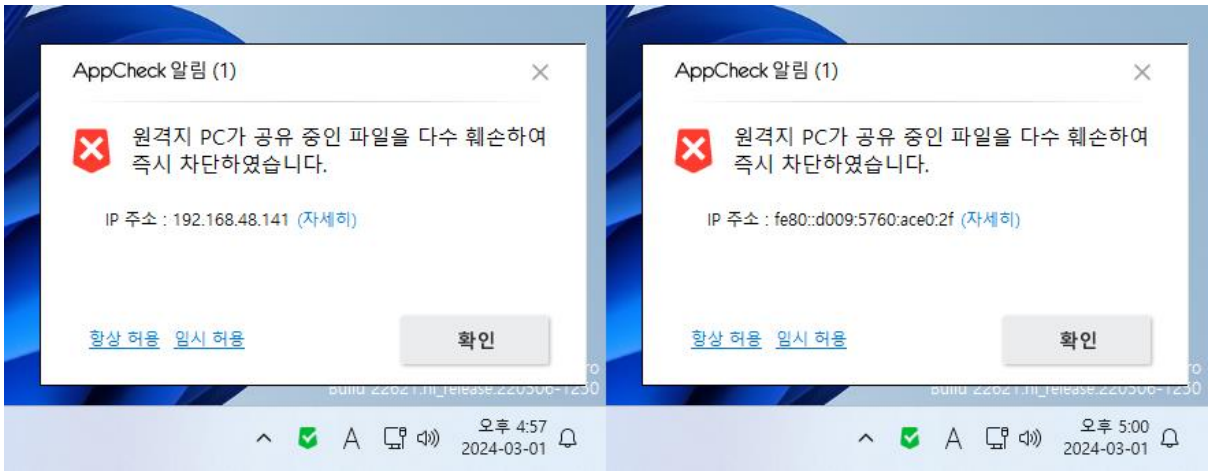
예외 폴더 목록에 추가된 항목 선택 후 삭제 시 "예외 폴더 목록에서 정말 삭제하시겠습니까?" 알림 메시지 창이 생성된다.



[7-7] SMB 목록

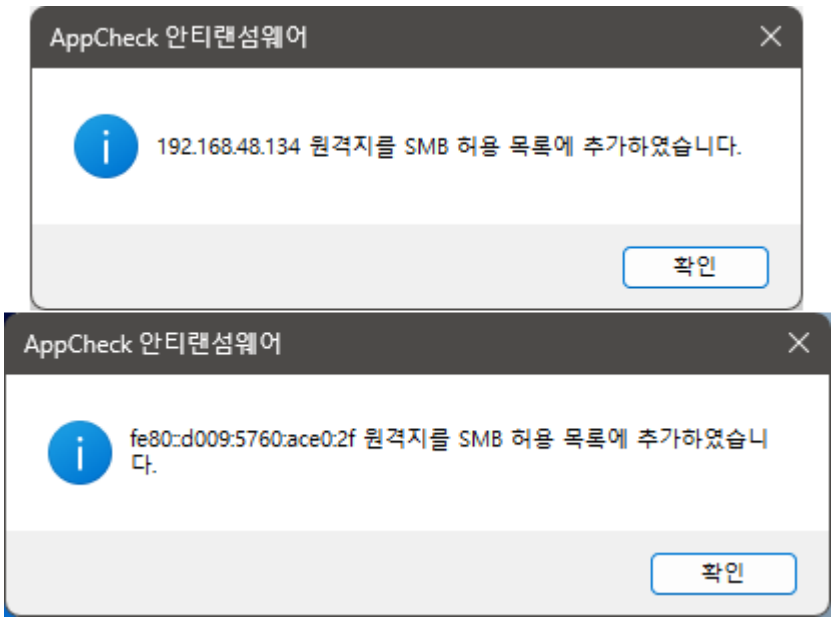


SMB 목록은 랜섬 가드의 "SMB 서버 보호" 기능을 위한 옵션이며, SMB 프로토콜로 연결된 네트워크 드라이브(공유 폴더) 내 보호할 파일을 원격지 PC에서 실행된 랜섬웨어에 의해 훼손 시 원격지 PC IP 주소(IPv4, IPv6)를 임시 차단(1시간 후 자동 해제) 및 허용할 수 있다.

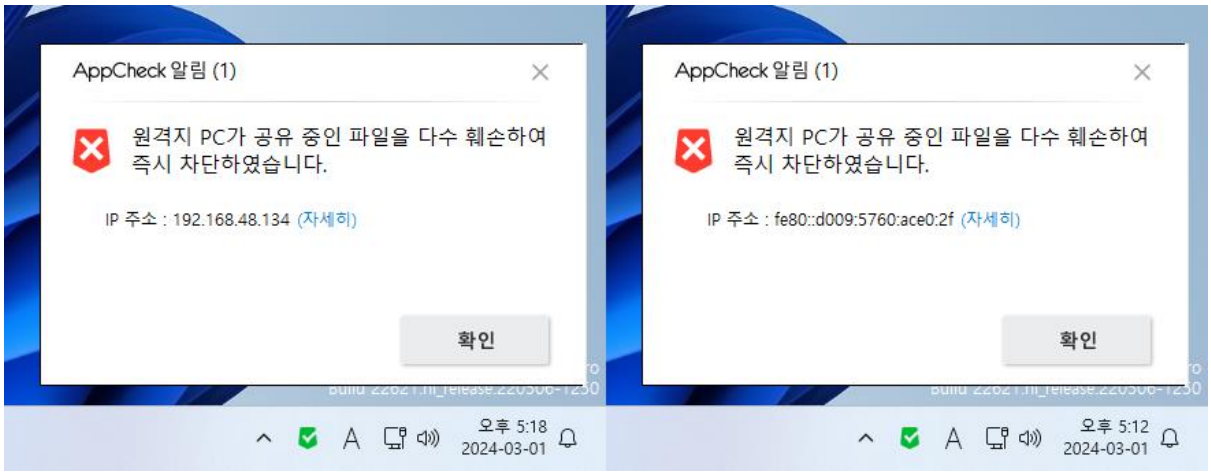


원격지 PC에서 실행된 랜섬웨어가 SMB 서버의 공유 폴더 내 파일 훼손 시 "원격지 PC가 공유 중인 파일을 다수 훼손하여 즉시 차단하였습니다." 알림창을 통해 원격지 IP 주소(랜섬웨어가 실행된 원격지 PC의 IP 주소)를 임시 차단 및 훼손된 파일을 자동 복원한다.

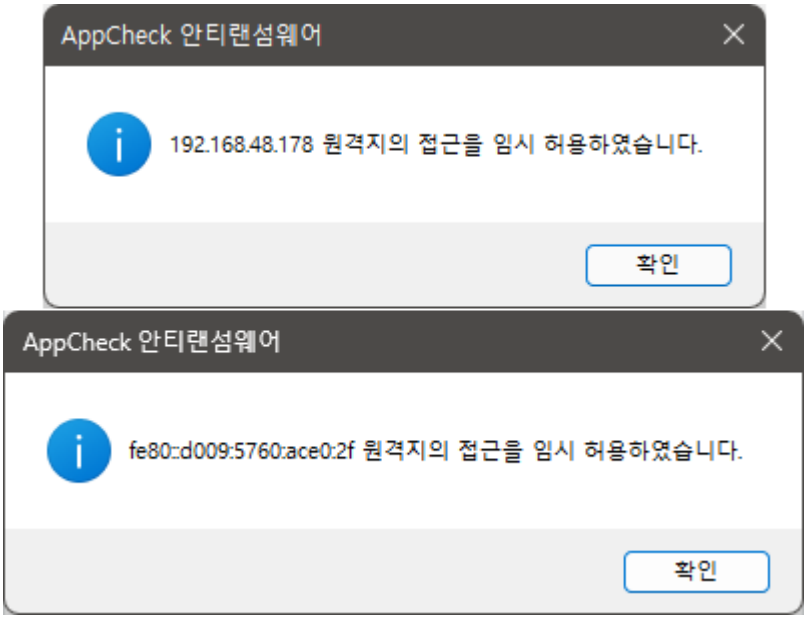
- **IP 주소 (자세히) :** "도구 – 위협 로그" 메뉴로 자동 연결
- **항상 허용 :** 차단된 원격지 IP 주소를 항상 허용 (옵션 – SMB 목록 – 허용된 주소 목록에 추가)



만약 "옵션 – 일반 - 잠금 설정 사용" 체크 또는 CMS 중앙 관리의 "정책 관리 - 일반 - Lock Mode (ON)" 설정인 경우 "항상 허용" 메뉴가 표시되지 않는다.



- **임시 허용 :** 차단된 원격지 IP 주소를 1회 임시 허용 (차단된 주소 목록에 추가된 원격지 IP 주소 삭제 처리)

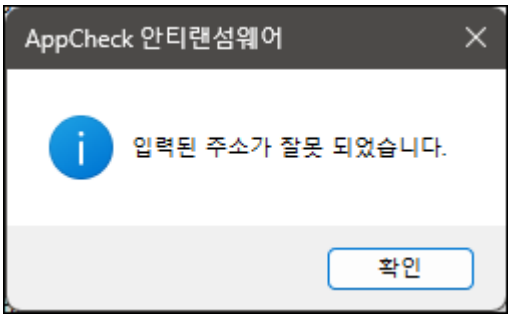


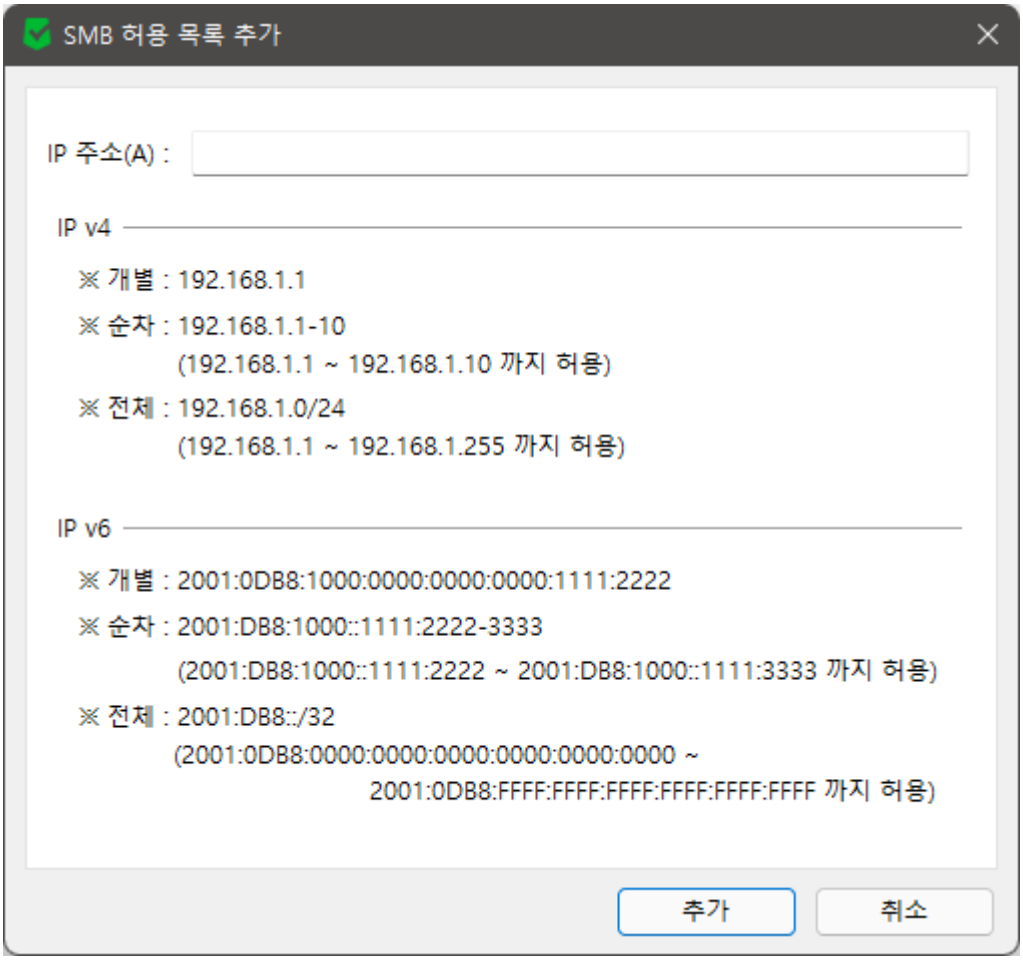
만약 "옵션 – 일반 - 잠금 설정 사용" 체크 또는 CMS 중앙 관리의 "정책 관리 - 일반 - Lock Mode (ON)" 설정인 경우 "임시 허용" 메뉴가 표시되지 않는다.

⊙ 허용된 주소 목록

"허용된 주소 목록"에 사용자가 직접 IP 주소를 추가하기 위해서는 "추가" 버튼을 클릭하여 IPv4 또는 IPv6 주소(단축 형식 허용)를 개별, 순차, 전체 규칙에 따라 특정 IP 주소 또는 IP 대역을 추가할 수 있다.

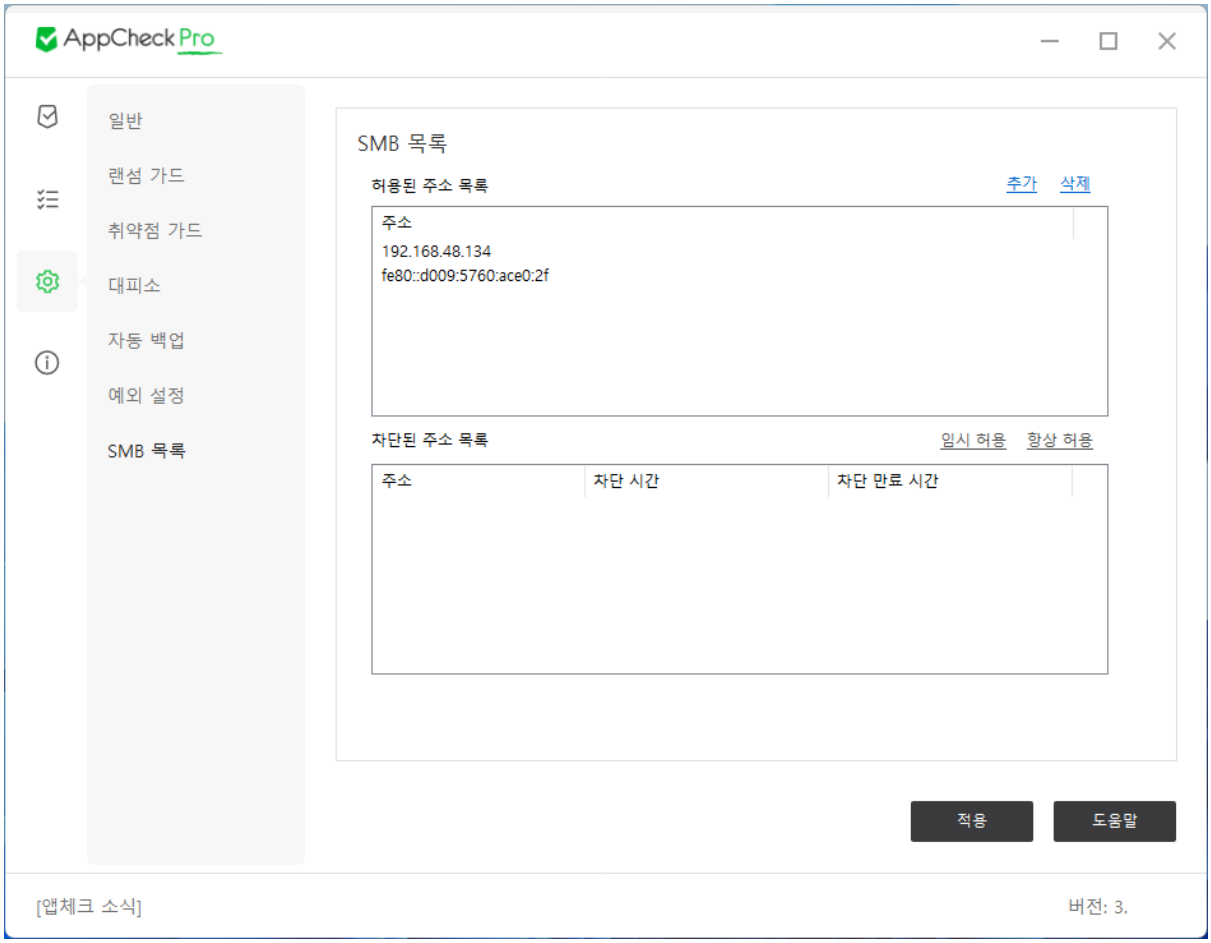
허용된 주소 목록에 허용하지 않는 IP 주소를 입력하여 추가할 경우 "입력된 주소가 잘못 되었습니다." 알림 메시지 창이 생성된다.



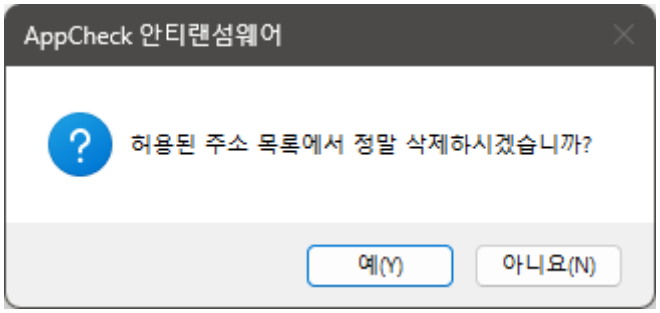


- **IP v4 주소 추가 규칙**
  - **개별 :** 192.168.1.1
  - **순차 :** 192.168.1.1-10 (192.168.1.1 ~ 192.168.1.10 까지 허용)
  - **전체 :** 192.168.1.0/24 (192.168.1.1 ~ 192.168.1.255 까지 허용)
- **IP v6 주소 추가 규칙**
  - **개별 :** 2001:0DB8:1000:0000:0000:0000:1111:2222
  - **순차 :** 2001:DB8:1000::1111:2222-3333 (2001:DB8:1000::1111:2222 ~ 2001:DB8:1000::1111:3333 까지 허용)
  - **전체 :** 2001:DB8::/32 (2001:0DB8:0000:0000:0000:0000:0000:0000 ~ 2001:0DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 까지 허용)

만약 허용된 주소 목록에 추가된 원격지 IP 주소를 통해 공유 폴더 내 파일 훼손 시 AppCheck 차단은 이루어지지 않지만 대피소 폴더에 백업은 이루어지므로 수동 복원을 할 수 있다.

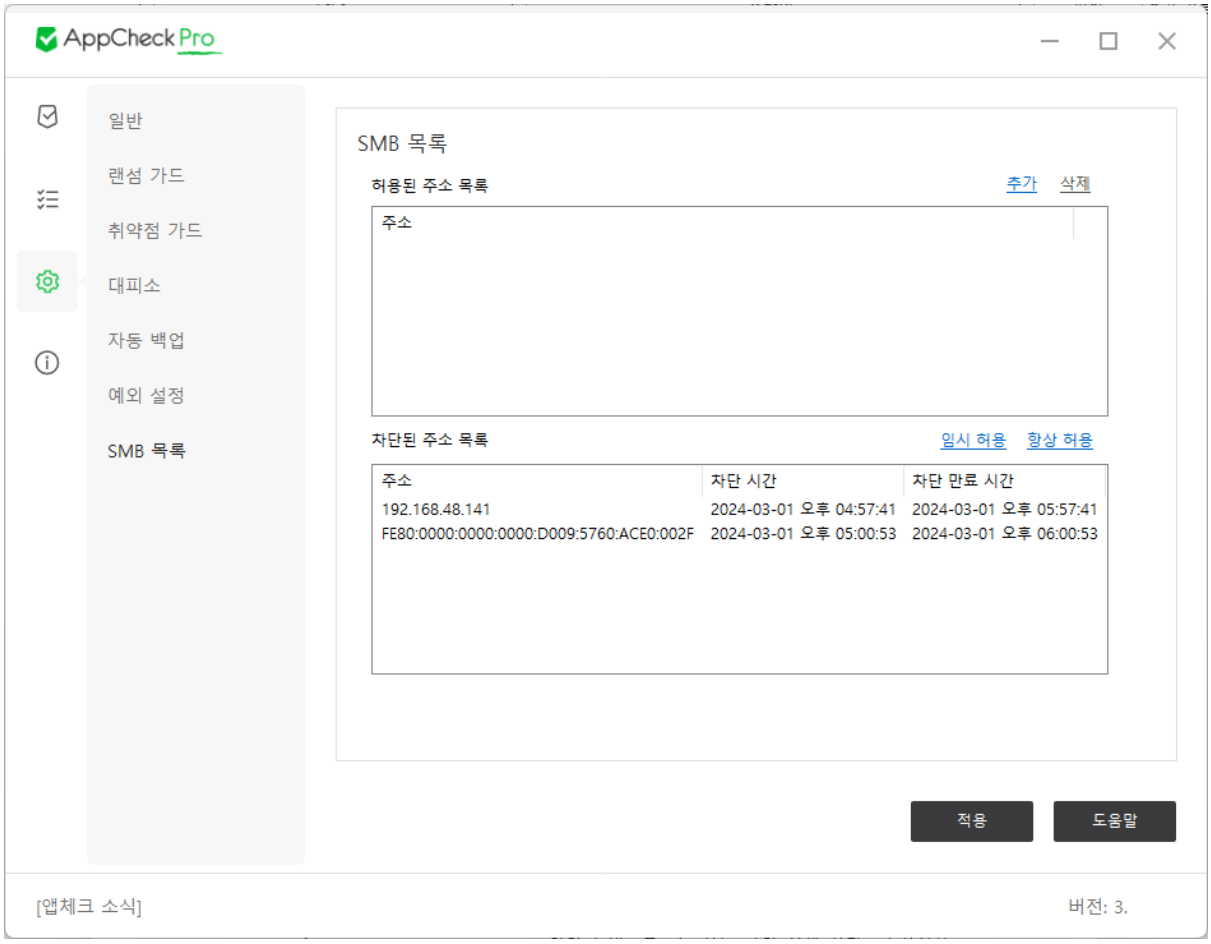


허용된 주소 목록에 추가된 IP 주소를 선택 후 삭제 시 "허용된 주소 목록에서 정말 삭제하시겠습니까?" 안내 메시지 창이 생성된다.



⊙ 차단된 주소 목록

"차단된 주소 목록"에 등록된 원격지 IP 주소는 1시간 동안 임시 차단되며 차단 만료 시간이 경과하면 자동으로 차단된 주소 목록에 등록된 IP 주소는 삭제 처리되어 차단되었던 원격지 PC에서 공유 폴더 내 파일에 대한 접근이 가능하다.

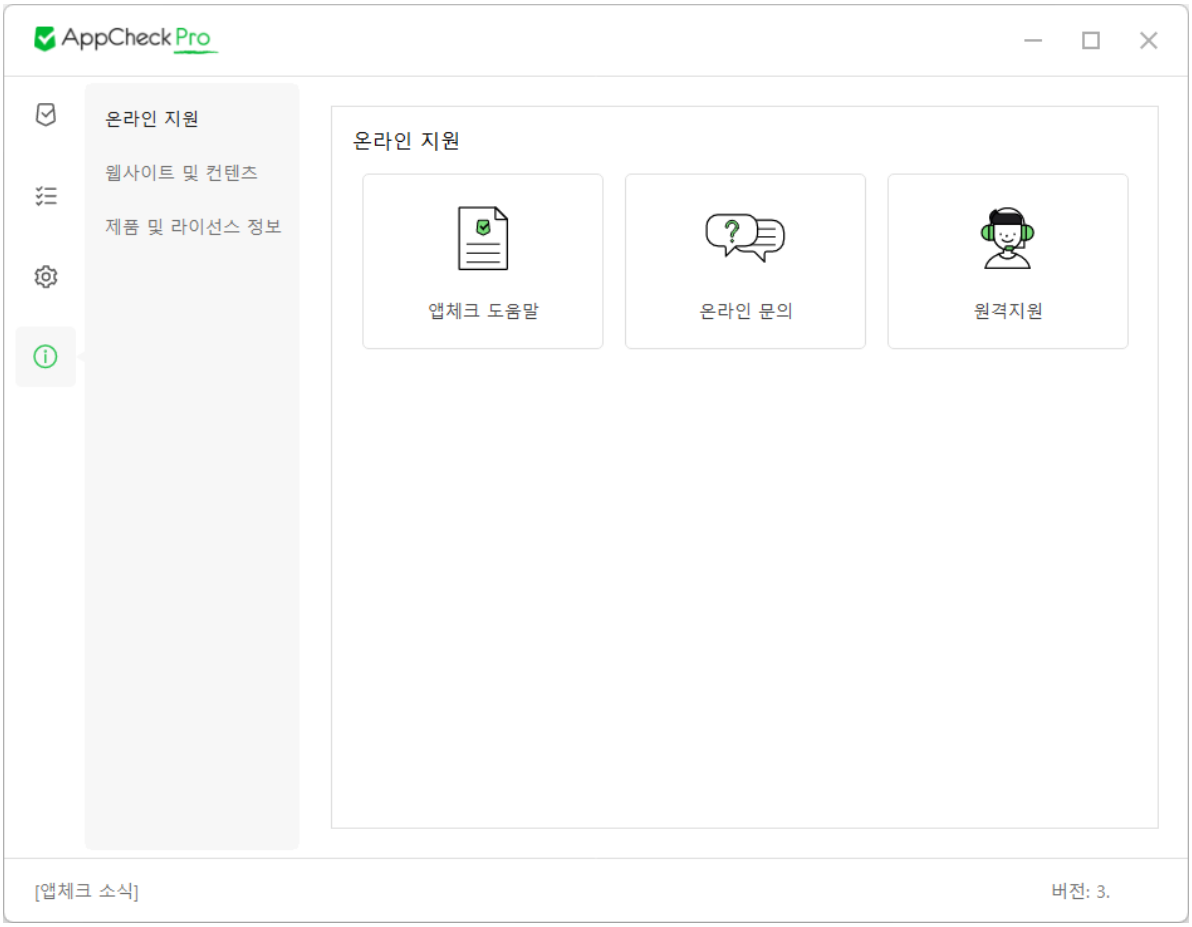


- **차단된 주소 목록 (임시 허용) :** 차단된 주소 목록에 등록된 원격지 IP 주소를 삭제하며, 삭제된 원격지 IP 주소를 통한 공유 폴더 내 파일 훼손 시 다시 차단한다.
- **차단된 주소 목록 (항상 허용) :** 차단된 주소 목록에 등록된 원격지 IP 주소를 "허용된 주소 목록"에 추가하여 해당 원격지 IP 주소에서 공유 폴더 내 파일 훼손 시 차단하지 않는다.
- **주소 :** 차단된 원격지 IP 주소 (IPv4 또는 IPv6)
- **차단 시간 :** 원격지 IP 주소가 차단된 시간
- **차단 만료 시간 :** 차단된 원격지 IP 주소가 자동 해제되는 시간 (차단 후 1시간)

만약 Windows 재부팅이 이루어질 경우 차단 만료 시간(1시간)과 상관없이 차단된 원격지 IP 주소는 자동 삭제된다.

8. AppCheck : 고객센터

[8-1] 온라인 지원

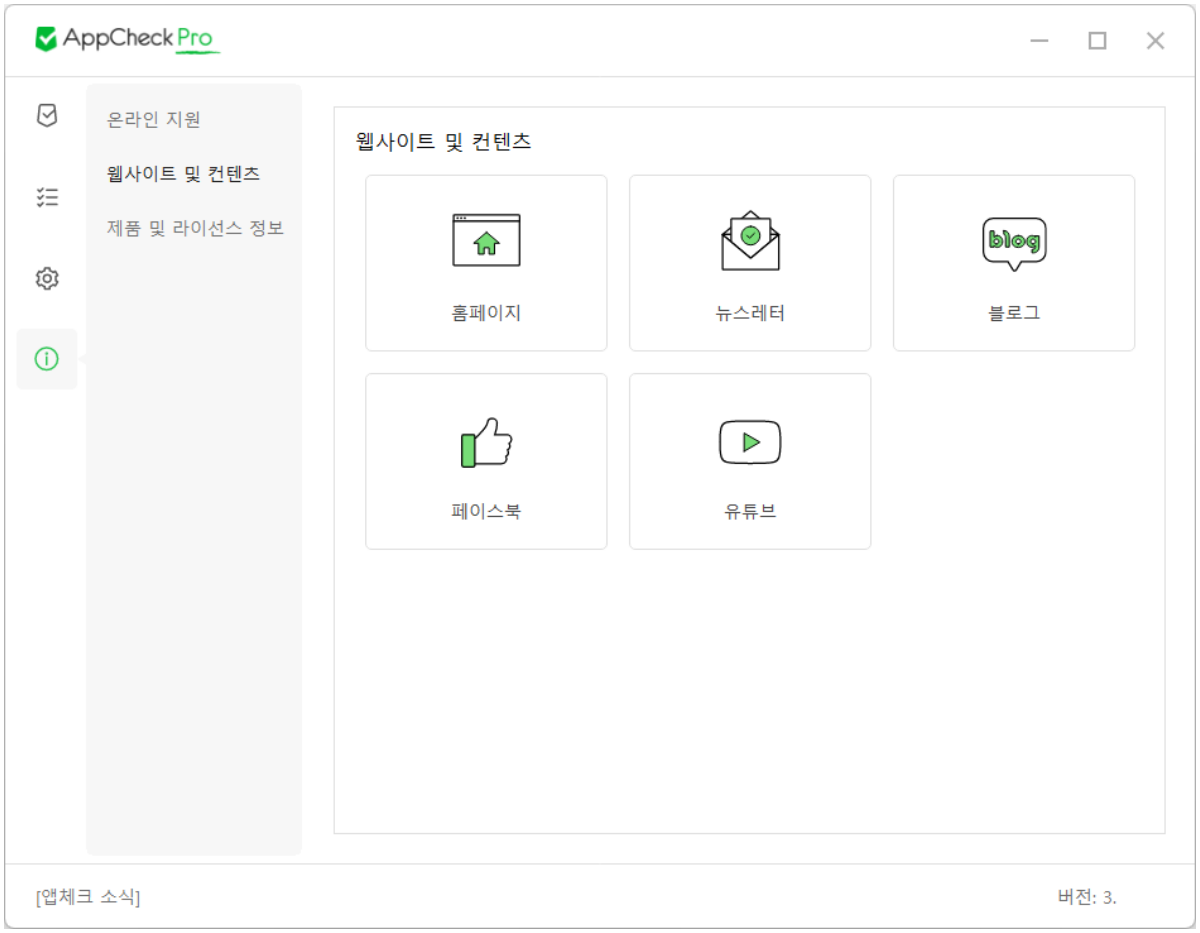


⊙ **앱체크 도움말 :** 체크멀 사이트에서 제공하는 온라인 매뉴얼 페이지 연결

⊙ **온라인 문의 :** 체크멀 사이트에서 제공하는 온라인 문의 페이지 연결

⊙ **원격지원 :** 체크멀 원격 지원 페이지 연결 (사전에 원격 지원 예약 필요)

[8-2] 웹사이트 및 컨텐츠



⊙ **홈페이지 :** 체크멀 메인 페이지 연결

⊙ **뉴스레터 :** 체크멀 사이트에서 제공하는 뉴스레터 페이지 연결

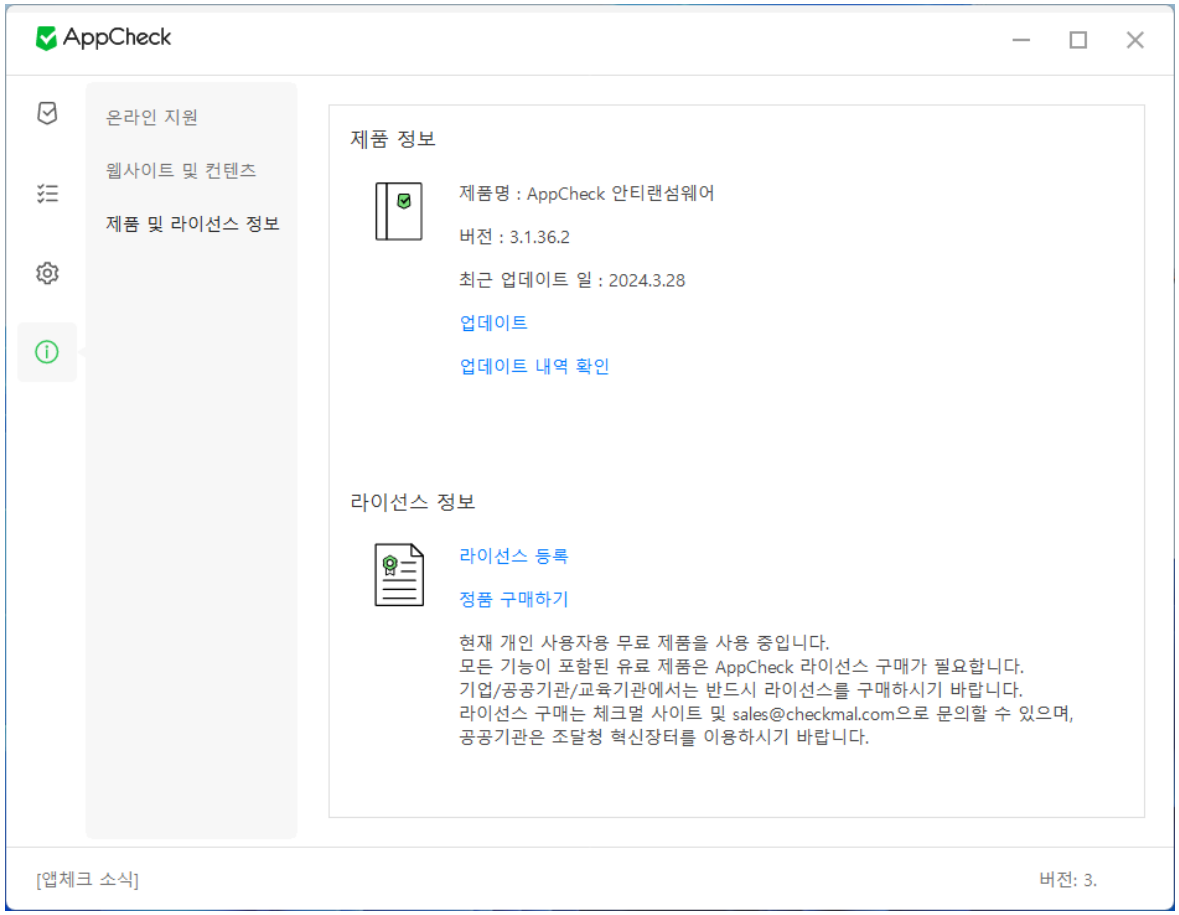
⊙ **블로그 :** 체크멀에서 운영하는 블로그 연결

⊙ **페이스북 :** 체크멀에서 운영하는 페이스북 계정 연결

⊙ **유튜브 :** 체크멀에서 운영하는 유튜브 계정 연결

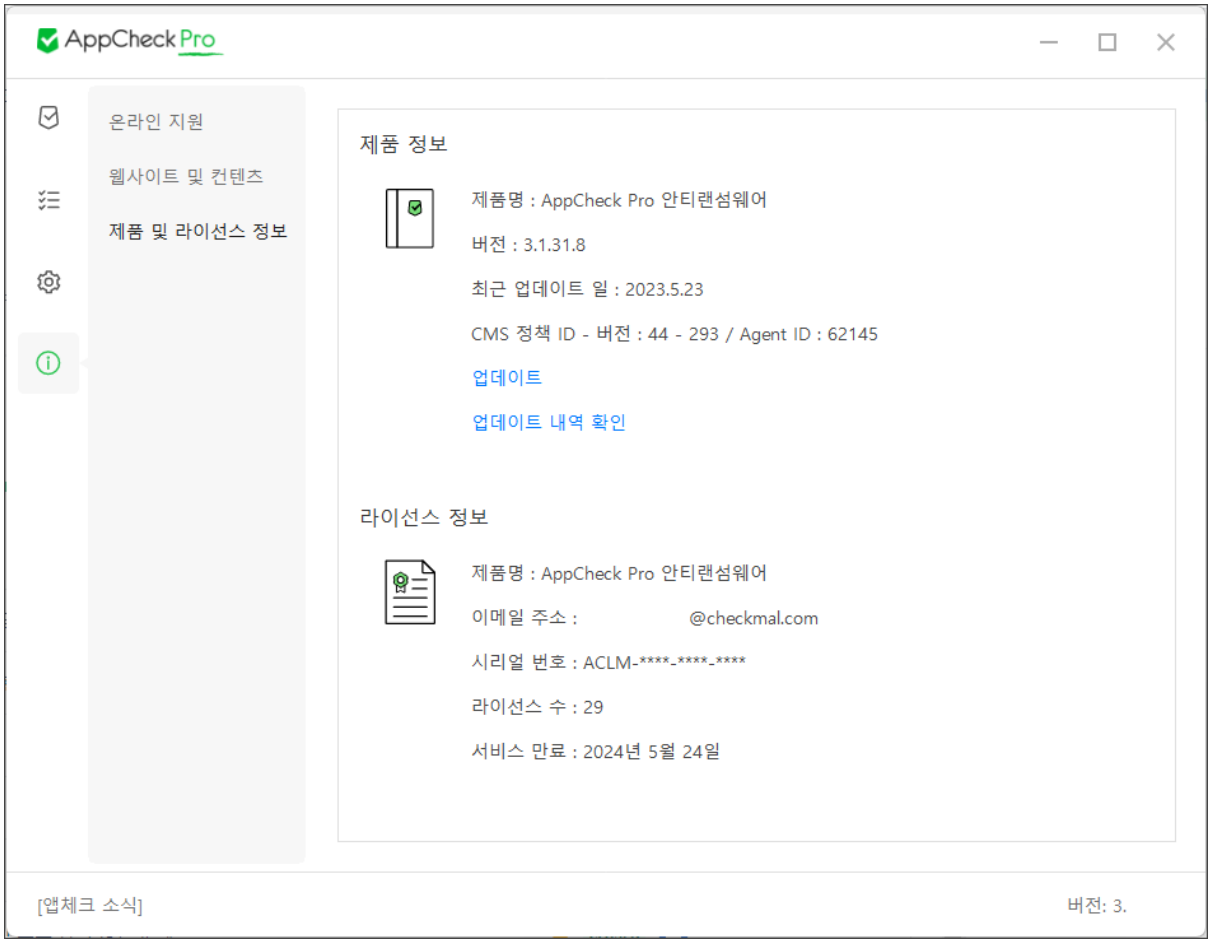
[8-3] 제품 및 라이선스 정보

⊙ 제품 정보



- **제품명 :** AppCheck 안티랜섬웨어 (개인 사용자용 무료 버전) 또는 AppCheck Pro 안티랜섬웨어 (유료 버전) 표시
- **버전 :** 설치된 AppCheck 빌드 버전 정보
- **최근 업데이트 일 :** 설치된 AppCheck 빌드 버전의 업데이트 날짜
- **업데이트 :** AppCheck 빌드 버전의 최신 업데이트 상태 확인
- **업데이트 내역 확인 :** 체크멀 "공지사항 – 릴리즈 노트" 게시물 연결

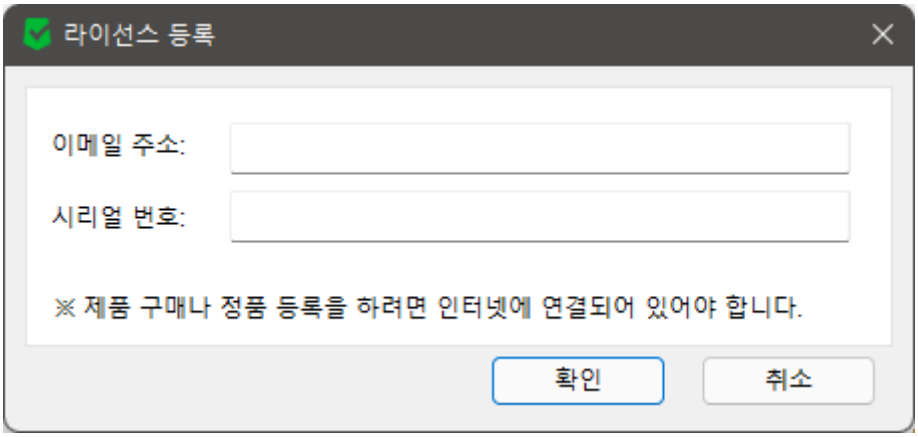
AppCheck Pro 안티랜섬웨어 제품 중 CMS 중앙 관리 연동 방식으로 설치된 AppCheck는 CMS 정책 ID 버전과 에이전트(Agent) ID 정보를 추가로 표시한다.



- **CMS 정책 ID – 버전 ::**설치된 AppCheck 에이전트에 적용된 CMS 정책 ID와 정책 리비전 정보
- **Agent ID :** 설치된 AppCheck 에이전트가 CMS 에이전트 리스트에 등록된 에이전트 ID

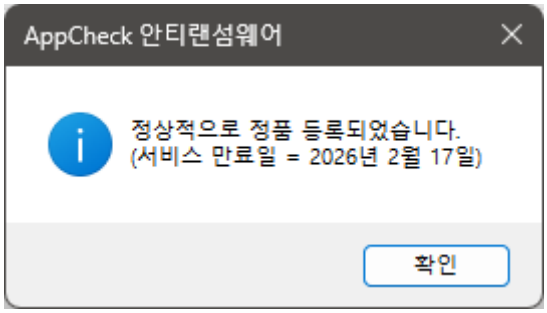
⊙ **라이선스 정보**

- **라이선스 등록 :** AppCheck Pro 정품 등록을 위한 이메일 주소와 시리얼 번호 입력



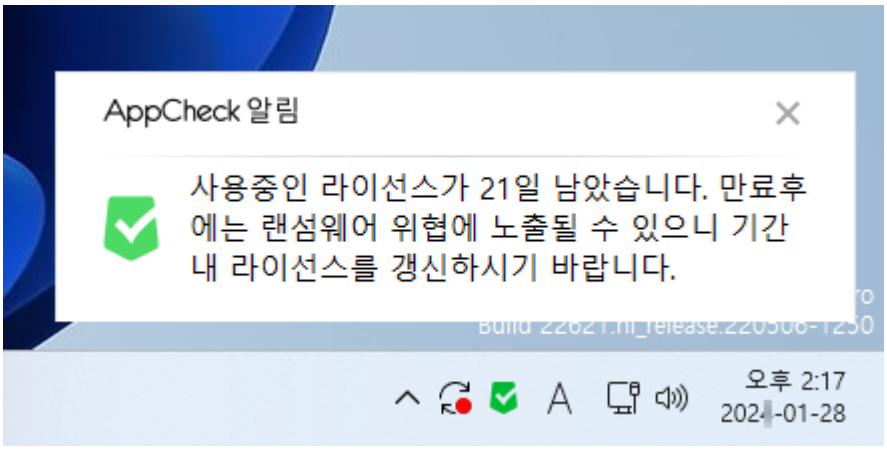
라이선스 등록 시에는 반드시 인터넷에 연결하여 체크멀 라이선스 서버와 통신이 이루어져야 한다. 단, CMS 중앙 관리 연동 제품은 최초 설치 시 AppCheck Pro 정품 등록이 이루어진 상태로 설치된다.

라이선스 등록이 성공적으로 이루어질 경우 "정상적으로 정품 등록되었습니다. (서비스 만료일 = 20○○년 ○월 ○일)" 알림 메시지 창이 표시된다.

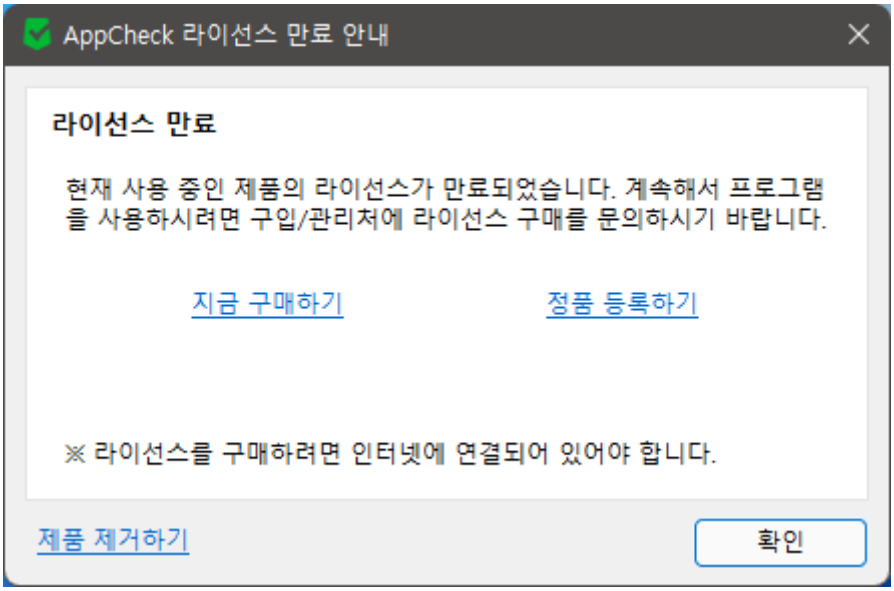


- **정품 구매하기 :** AppCheck Pro 개인 구매 페이지 연결
- **제품명 :** AppCheck Pro 안티랜섬웨어
- **이메일 주소 :** 라이선스 이메일 주소
- **시리얼 번호 :** 라이선스 시리얼 번호 (맨 앞자리 4자리만 표시)
- **라이선스 수 :** 라이선스로 설치 가능한 장치 수
- **서비스 만료 :** 라이선스의 서비스 만료일

AppCheck Pro 라이선스 만료 31 일 전부터 "사용중인 라이선스가 ○○일 남았습니다. 만료후에는 랜섬웨어 위협에 노출될 수 있으니 기간내 라이선스를 갱신하시기 바랍니다." 알림 메시지가 3 일 주기로 1 일 1 회 생성된다. 단, CMS 중앙 관리 연동 제품은 AppCheck Pro 라이선스 만료 사전 알림 메시지가 생성되지 않는다.



AppCheck Pro 라이선스 만료 시 모든 기능이 종료되며, 제품 실행 시 "AppCheck 라이선스 만료 안내"를 통해 "현재 사용 중인 제품의 라이선스가 만료되었습니다. 계속해서 프로그램을 사용하시려면 구입/관리처에 라이선스 구매를 문의하시기 바랍니다." 안내 메시지 창이 생성된다.



- **지금 구매하기 :** AppCheck 라이선스 갱신 페이지 연결
- **정품 등록하기 :** AppCheck 라이선스 등록창 생성을 통해 구매한 라이선스 이메일 주소와 시리얼 번호 등록
- **제품 제거하기 :** AppCheck 삭제하기

AppCheck 라이선스 만료창이 뜬 상태에서 기존 라이선스 정보 그대로 갱신을 한 경우 시스템 재부팅 또는 AppCheck 시스템 트레이 아이콘 더블 클릭 시 갱신된 라이선스 만료창이 종료되며 라이선스 갱신이 이루어진다. 단, 잠금 설정 사용 환경에서는 잠금 설정 해제 후 실시간 보호를 다시 활성화해야 한다.