AhnLab

내 PC 지키미

에이전트 사용설명서

AhnLab

목차

일러 두기

내 PC 지키미 사용설명서의 내용과 프로그램은 저작권법과 컴퓨터프로그램보호법에 의해서 보호받고 있습니다.
이 사용설명서에 표기된 제품명은 각 사의 등록상표입니다.

사용설명서 버전: **2017.04.27** / 제품 버전: **4.6.7**

면책 조항

제조자, 수입자, 대리점은 상해를 포함하는 우발적인 손상 또는 본 제품의 부적절한 사용과 조작으로 인한 기타 손상에 대해 책임을 지지 않습니다. 사용설명서의 내용은 현재 제품을 기준으로 작성되었습니다. (주)안랩은 지금도 새로운 기능을 추가 보완하고 있으며 향후에도 지속적으로 새로운 기술을 적용할 것입니다. 제품의 모든 기능은 제품 구입자 또는 제품 구입 기업에게 사전 통보없이 변경될 수 있으며 이 사용설명서의 내용과 차이가 날 수 있습니다.

표기 규칙

문서의 이해를 위해 기본적으로 알아둬야 할 표기 규칙은 다음과 같습니다.

표기 규칙	내용
<창 이름>	웹 브라우저에 표시되는 창의 이름을 나타냅니다.
굵은 글꼴	제품 화면에서 볼 수 있는 항목 이름, 또는 메시지를 나타냅니다. (예: 로그온할 **ID** 와 **비밀번호**를 입력하고 **로그온**을 누릅니다.)
PC 점검 > 점검 시작	'>'이 포함된 굵은 글꼴은 메뉴 실행 경로를 나타냅니다.
참고	제품을 사용할 때 참고할 사항입니다.
주의	제품을 사용할 때 주의해야 할 사항입니다.
내 PC 지키미	AhnLab 내 PC 지키미를 줄여서 **내 PC 지키미**로 표기합니다.
제품	AhnLab 내 PC 지키미를 구성하는 모든 요소를 **제품**으로 표기합니다.
에이전트	AhnLab 내 PC 지키미 Agent 를 **에이전트**로 표기합니다.
관리 콘솔	AhnLab 내 PC 지키미 Agent 를 관리하는 AhnLab 내 PC 지키미 Admin 을 **관리 콘솔**로 표기합니다.
APM	AhnLab Patch Management 를 줄여서 **APM** 으로 표기합니다.

오픈소스

본 제품에서 사용된 오픈소스 관련 정보는 http://opensource.ahnlab.com 에서 확인할 수 있습니다.

고객지원 연락처

- 홈페이지: http://www.ahnlab.com
- 등록고객 온라인 문의: http://www.ahnlab.com 의 고객지원 > 1:1 상담
- 주소: 경기도 성남시 분당구 판교역로 220 (우)13493

구매 문의

- 전화 번호: 1588-3096
- 운영 시간: 평일 오전 9 시 ~ 오후 6 시 (토, 공휴일 제외)
- 제품 정보: http://www.ahnlab.com 의 제품 구매 > 구매처 안내

기업고객 기술지원

- 전화 번호: 1577-9431
- 운영 시간: 평일 오전 9 시 ~ 오후 8 시 (토, 공휴일 제외)
- 팩스: 031-722-8901

1 장

설치 하기

시스템 사양

내 PC 지키미 에이전트의 사용 환경입니다.

에이전트 사용 환경

내 PC 지키미 에이전트를 설치하기 위한 시스템 사양은 다음과 같습니다.

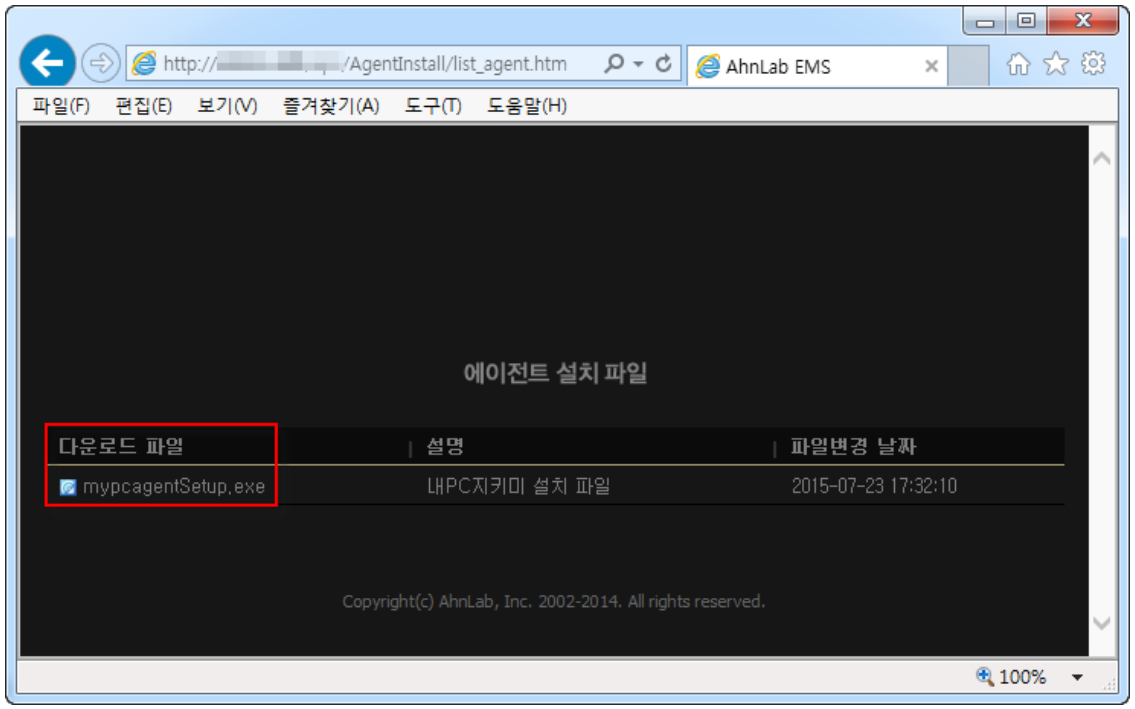
- 64 비트는 32 비트 호환 모드로 지원하고, IA64 시스템은 지원하지 않습니다.
- Server Core Install 모드는 지원하지 않습니다.

시스템 종류		Windows 버전
운영 체제 시스템 종류	32 비트	Microsoft Windows XP Professional(SP2 이상) Microsoft Windows XP Home(SP2 이상) Microsoft Windows XP Media Center(SP2 이상) Microsoft Windows Server 2003 R2 Standard(SP1 이상) Microsoft Windows Server 2003 R2 Enterprise(SP1 이상) Microsoft Windows Server 2003 R2 Datacenter(SP1 이상) Microsoft Windows Server 2003 R2 Web(SP1 이상)
	64 비트	Microsoft Windows XP Professional x64 Microsoft Windows Server 2003 R2 Standard x64 Microsoft Windows Server 2003 R2 Enterprise x64 Microsoft Windows Server 2003 R2 Datacenter x64
	32/64 비트 모두 지원	Microsoft Windows Vista Home Basic K/KN Microsoft Windows Vista Home Premium K Microsoft Windows Vista Business K Microsoft Windows Vista Enterprise Microsoft Windows Vista Ultimate K Microsoft Windows Server 2008 Standard Microsoft Windows Server 2008 Enterprise Microsoft Windows Server 2008 Datacenter Microsoft Windows Server 2008 Web Server Microsoft Windows Server 2008 R2 Standard Microsoft Windows Server 2008 R2 Enterprise Microsoft Windows Server 2008 R2 Datacenter Microsoft Windows Server 2008 R2 Web Server Microsoft Windows 7 Home Premium Microsoft Windows 7 Professional Microsoft Windows 7 Ultimate Microsoft Windows 8 Microsoft Windows 8.1 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2 Microsoft Windows 10 Pro Microsoft Windows 10 Enterprise Microsoft Windows 10 Education Microsoft Windows Server 2016

에이전트 설치하기

관리자가 공지한 내 PC 지키미 설치 파일을 사용자 PC 에 다운로드 하여 설치합니다. 설치된 내 PC 지키미를 실행하여 PC 를 점검할 수 있습니다.

1. 관리자가 공지한 웹사이트에서 내PC지키미 설치 파일을 다운로드 합니다.



2. 다운로드 한 내PC지키미 설치 파일을 실행합니다. 설정에 따라 설치 진행 과정이 화면에 표시되거나 표시되지 않을 수 있습니다.
3. 설치를 마치면 작업 표시줄에 내PC지키미 에이전트 아이콘()이 표시됩니다.

참고

내 PC 지키미 에이전트는 사용자가 임의로 삭제할 수 없습니다. 반드시 삭제를 해야 하는 경우에는 관리자에게 삭제 방법을 문의하시기 바랍니다.

2 장

시작 하기

보안 점검
보안 점검의 날
패스워드 안전성 검사

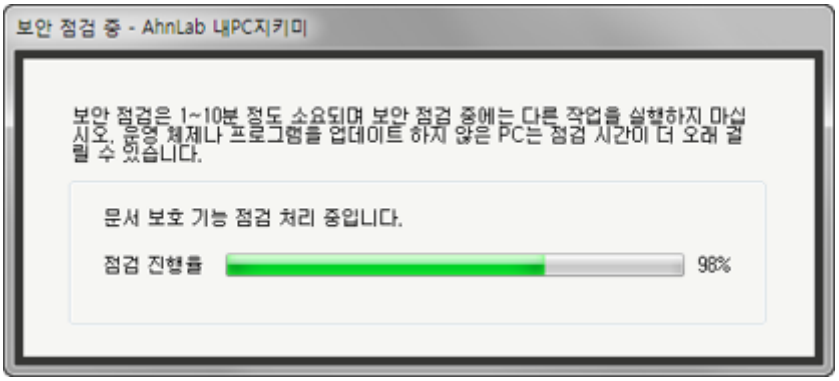
보안 점검

내 PC 지키미를 실행한 후에는 보안 점검을 해야 합니다. 보안 점검을 실행하면, PC 의 취약점을 점검하여 점검 항목별로 안전, 취약, 점검 불가 항목에 대한 정보를 확인할 수 있습니다.

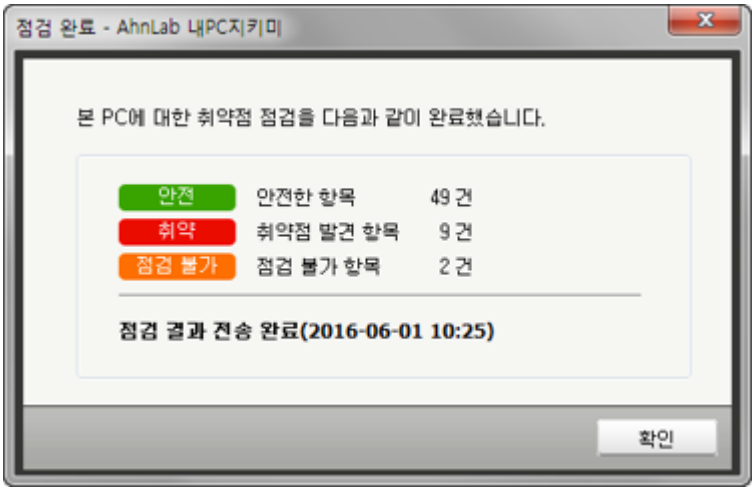
점검 방법

1. 바탕 화면의 내PC지키미 아이콘을 더블 클릭합니다.
2. 실행된 <AhnLab 내PC지키미>의 HOME 화면에서 **점검 시작**을 누릅니다.

3. 보안 점검 진행 화면이 나타납니다. 보안 점검은 사용자 PC 환경에 따라 1~10분 정도 소요됩니다.



4. <점검 완료>가 나타나면 안전, 취약, 점검 불가 항목에 대한 결과를 확인할 수 있습니다.



5. **확인**을 누르면 창이 닫힙니다.

참고

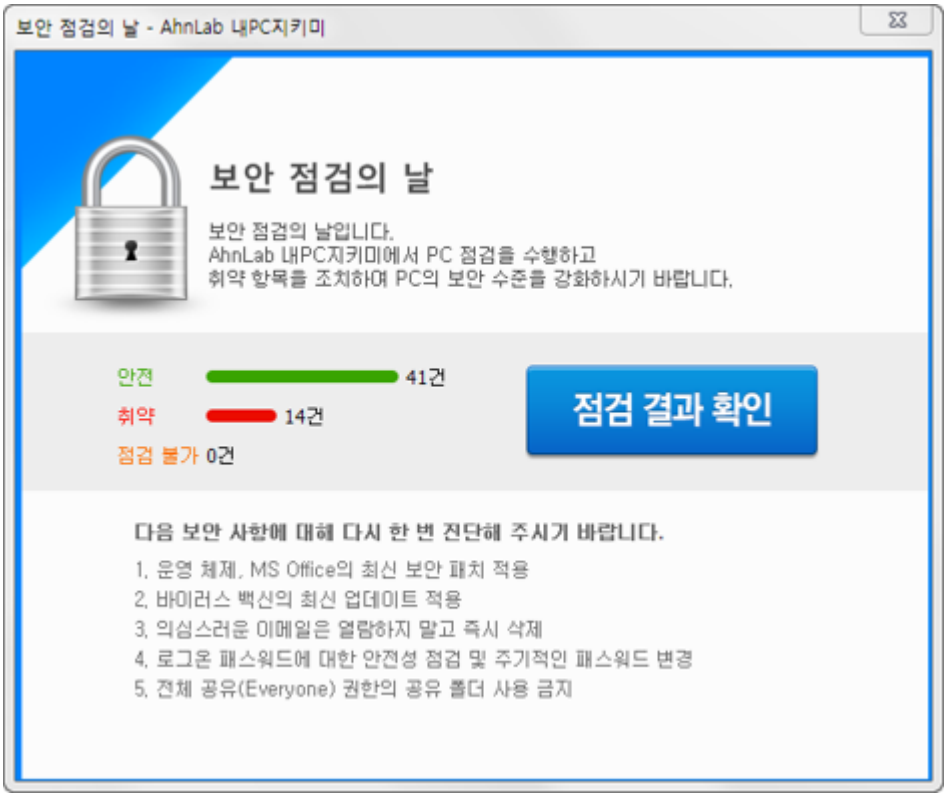
안전, 취약, 점검 불가 항목에 대한 상세 내용은 PC 점검에서 점검 결과를 확인하고 결과에 따른 조치를 취할 수 있습니다.

보안 점검의 날

내 PC 지키미가 설치된 PC 에서 관리자가 설정한 날짜에 컴퓨터를 시작하면 PC 점검이 자동으로 실행됩니다.

점검 방법

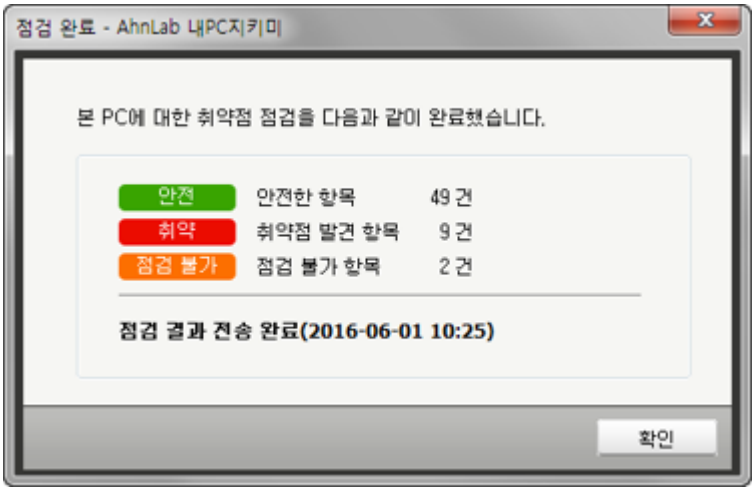
1. 보안 점검의 날 알림 화면이 표시된 후 자동으로 PC 점검을 시작합니다.



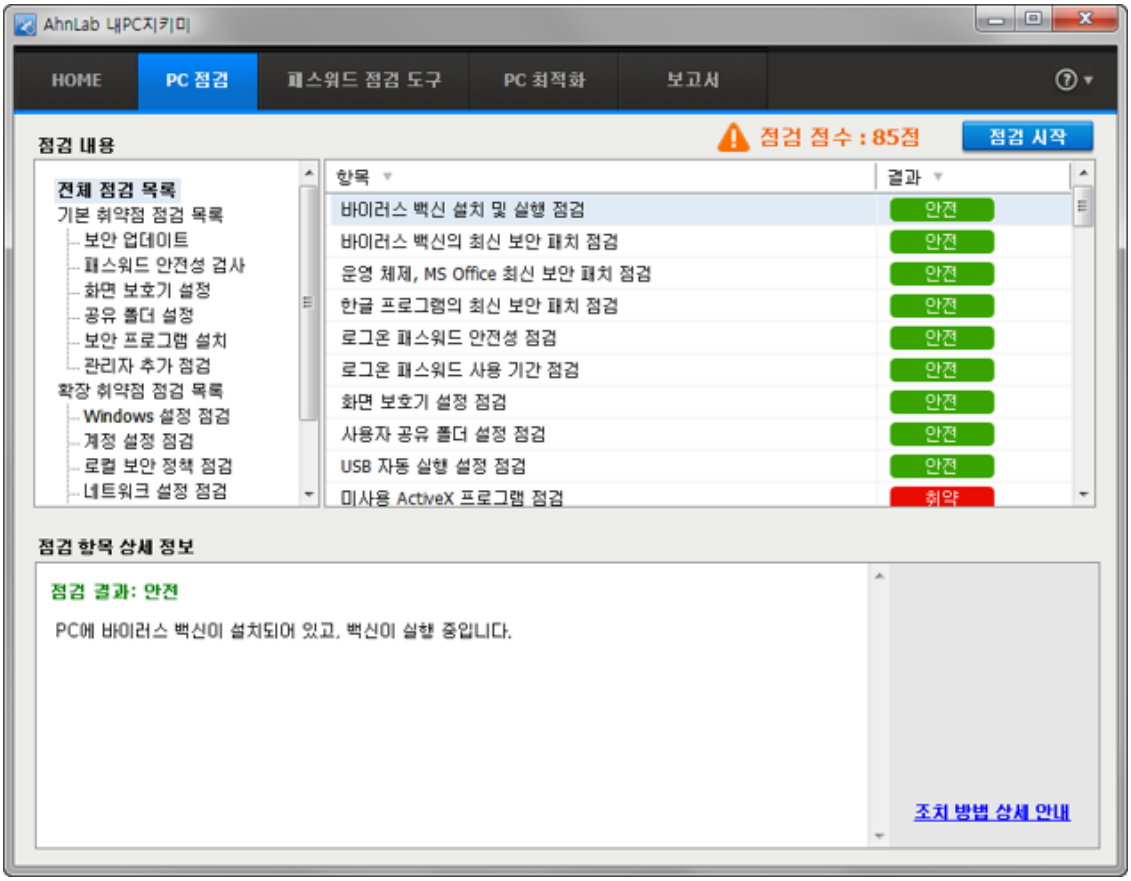
참고

보안 점검의 날에는 점검 시작 버튼을 누르지 않아도 자동으로 PC 점검을 시작합니다.

2. 점검을 마치면 표시되는 <점검 완료>에서 안전, 취약, 점검 불가 항목을 확인합니다.



3. 점검 결과에 대한 상세 내용을 확인하려면 내PC지키미의 **PC 점검** 탭에서 점검 결과를 확인하여 필요한 조치를 취합니다.

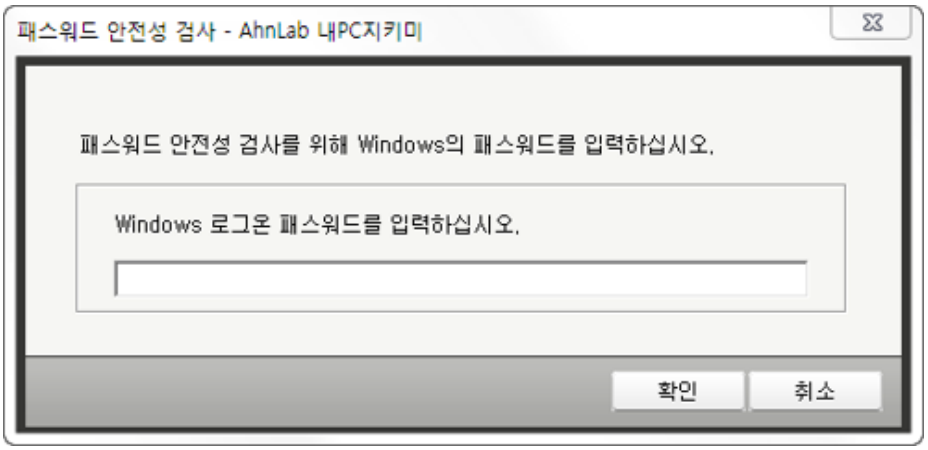

AhnLab 내PC지키미
HOME
PC 점검
패스워드 점검 도구
PC 최적화
보고서
점검 내용
점검 점수 : 85점
점검 시작
전체 점검 목록
기본 취약점 점검 목록
보안 업데이트
패스워드 안전성 검사
화면 보호기 설정
공유 폴더 설정
보안 프로그램 설치
관리자 추가 점검
확장 취약점 점검 목록
Windows 설정 점검
계정 설정 점검
로컬 보안 정책 점검
네트워크 설정 점검
항목
결과
바이러스 백신 설치 및 실행 점검 안전
바이러스 백신의 최신 보안 패치 점검 안전
운영 체제, MS Office 최신 보안 패치 점검 안전
한글 프로그램의 최신 보안 패치 점검 안전
로그온 패스워드 안전성 점검 안전
로그온 패스워드 사용 기간 점검 안전
화면 보호기 설정 점검 안전
사용자 공유 폴더 설정 점검 안전
USB 자동 실행 설정 점검 안전
미사용 ActiveX 프로그램 점검 취약
점검 항목 상세 정보
점검 결과: 안전
PC에 바이러스 백신이 설치되어 있고, 백신이 실행 중입니다.
조치 방법 상세 안내

패스워드 안전성 검사

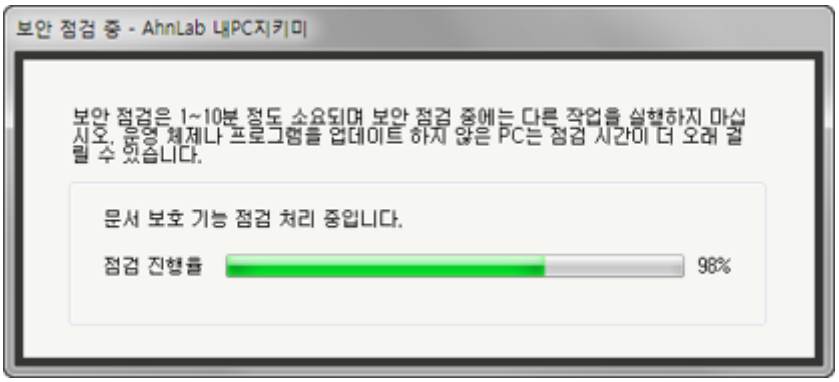
패스워드 안전성 검사는 내 PC 지키미를 처음 실행했거나, Windows 계정의 비밀번호가 변경되었을 경우 실행됩니다.

점검 방법

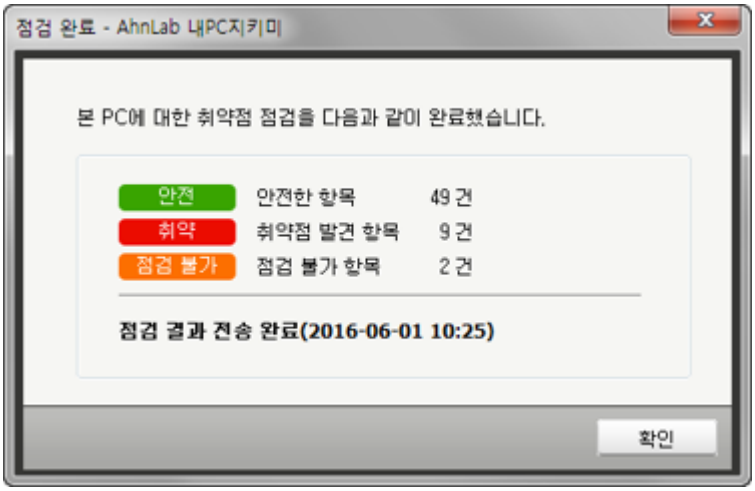
1. 바탕 화면의 내PC지키미 아이콘을 더블 클릭합니다.
2. 내PC지키미를 처음 실행했거나, Windows 계정의 비밀번호를 변경한 경우 <패스워드 안전성 검사>가 나타납니다.
3. 패스워드 입력란에 Windows 로그온 패스워드를 입력합니다.



4. 보안 점검 진행 화면이 나타납니다.

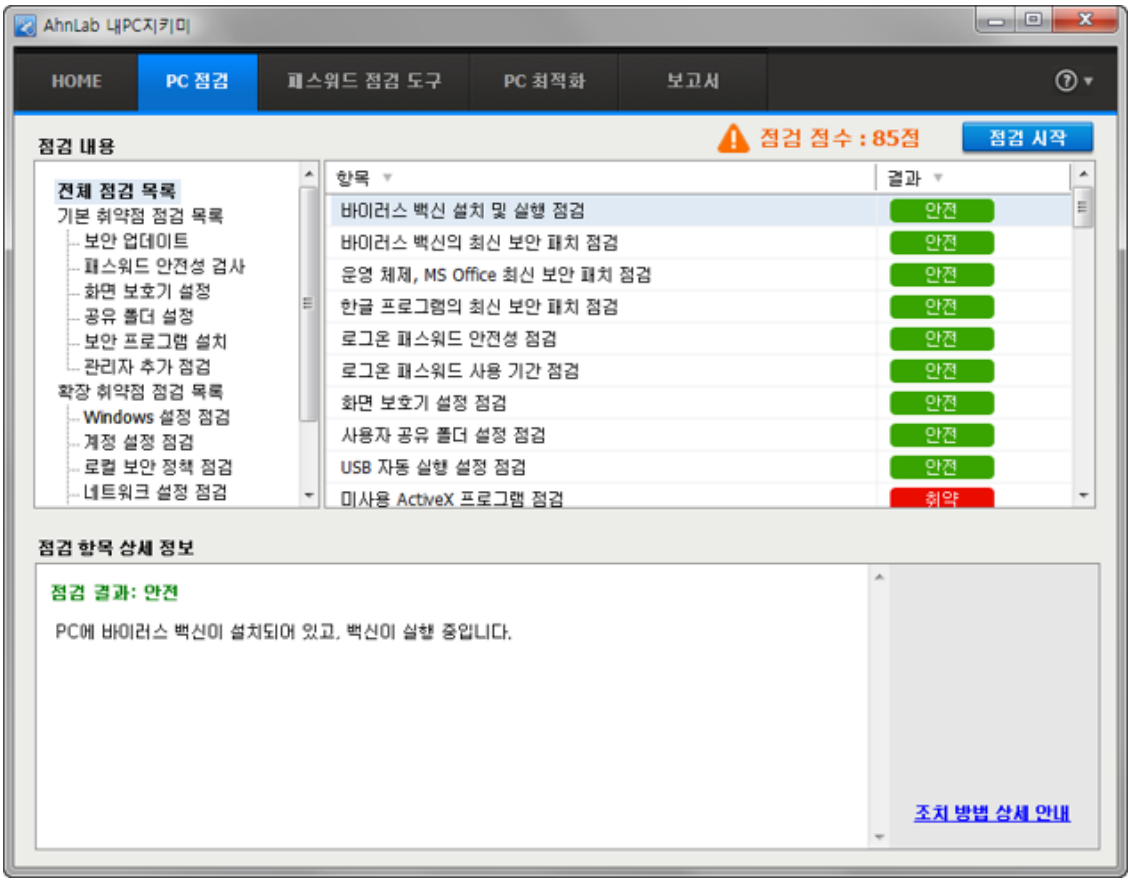


5. <점검 완료>가 나타나면, 안전, 취약, 점검 불가 항목에 대한 건수를 확인합니다.



6. **확인**을 누르면 창이 닫힙니다.

7. 내PC지키미의 **PC 점검** 탭에서 취약점 점검 결과를 확인합니다.



참고

패스워드 안전성 검사 항목은 다음과 같습니다.

- 입력한 패스워드가 Windows 로그온 비밀번호와 동일한 지 점검
- 입력한 패스워드가 Windows 로그온 계정 이름과 동일한지 점검
- 로그온 패스워드의 길이 및 필수문자 조합이 안전 조건을 준수하는지 점검
- 패스워드에 연속된 문자나 숫자의 포함 여부 점검

3 장

HOME

HOME

HOME 화면에서는 PC 점검을 시작할 수 있으며, 최근의 PC 점검 및 PC 최적화를 수행한 날짜를 확인할 수 있습니다.

상세 설명

HOME 화면은 다음과 같이 PC 점검을 시작할 수 있는 **점검 시작, PC 점검 점수 반영 항목, 최근 점검 결과, 점검 점수 추이, PC 최적화 날짜**로 구성되어 있습니다.

점검 시작

PC 점검을 한 번도 수행하지 않는 경우는 점검 시작 버튼이 **미 점**검으로 나타납니다. PC 점검이 완료되면 점검 시작 버튼 위에 최근의 PC 점검 점수가 보여집니다.

PC 점검 점수 반영 항목

PC 점검 점수에 반영되는 항목은 관리자가 지정하여 설정할 수 있습니다.

최근 점검 결과

PC 점검을 수행한 점검 날짜와 점검 결과 전송 여부를 나타냅니다.

- 결과 전송 완료: PC 점검 결과가 관리자 서버로 정상적으로 전송 완료한 경우입니다.
- 결과 전송 중: PC 점검 결과가 관리자 서버로 전송중임을 나타냅니다.

점검 결과

보안 점검을 실행하면 점검 결과를 **안전, 취약, 점검 불가**로 표시합니다. 점검 결과가 안전이 아닌 경우에는 각 항목을 선택하여 점검 결과 상세 보기를 통해 취약하거나 점검이 불가한 이유를 확인할 수 있습니다.

- **안전**: 점검 결과 해당 항목의 문제점이 발견되지 않은 경우입니다. 안전으로 진단된 경우에는 녹색으로 해당 항목의 안전을 표시합니다.
- **취약**: 점검 결과 해당 항목이 보안상의 문제점이 있는 경우 취약으로 판정합니다. 취약으로 진단된 경우에는 빨간색으로 해당 항목의 위험을 알립니다. 취약으로 점검된 항목을 선택하여 각 항목별로 보안 센터 실행, 화면 보호기 설정 등의 조치를 실행하십시오.
- **점검 불가**: 점검 결과 해당 항목을 점검할 수 없는 경우에는 점검 불가로 판정합니다. 점검 불가로 진단된 경우에는 주황색으로 점검 불가를 알립니다. 점검 불가로 진단된 항목을 선택하여 각 항목의 점검 불가 사유를 확인하십시오.

점검 점수 추이

최근 5 회 동안 PC 점검 날짜와 점검 결과의 점수 추이를 그래프로 표시합니다.

PC 최적화 날짜

PC 최적화를 수행한 날짜를 나타냅니다. 한 번도 최적화를 수행하지 않은 경우는 PC 최적화를 실행할 수 있는 링크가 나타납니다.

다음 점검 일까지 남은 날짜

다음 PC 점검 일까지의 남은 날짜를 나타냅니다.

4 장

PC 점검

PC 점검
기본 취약점 진단
확장 취약점 진단

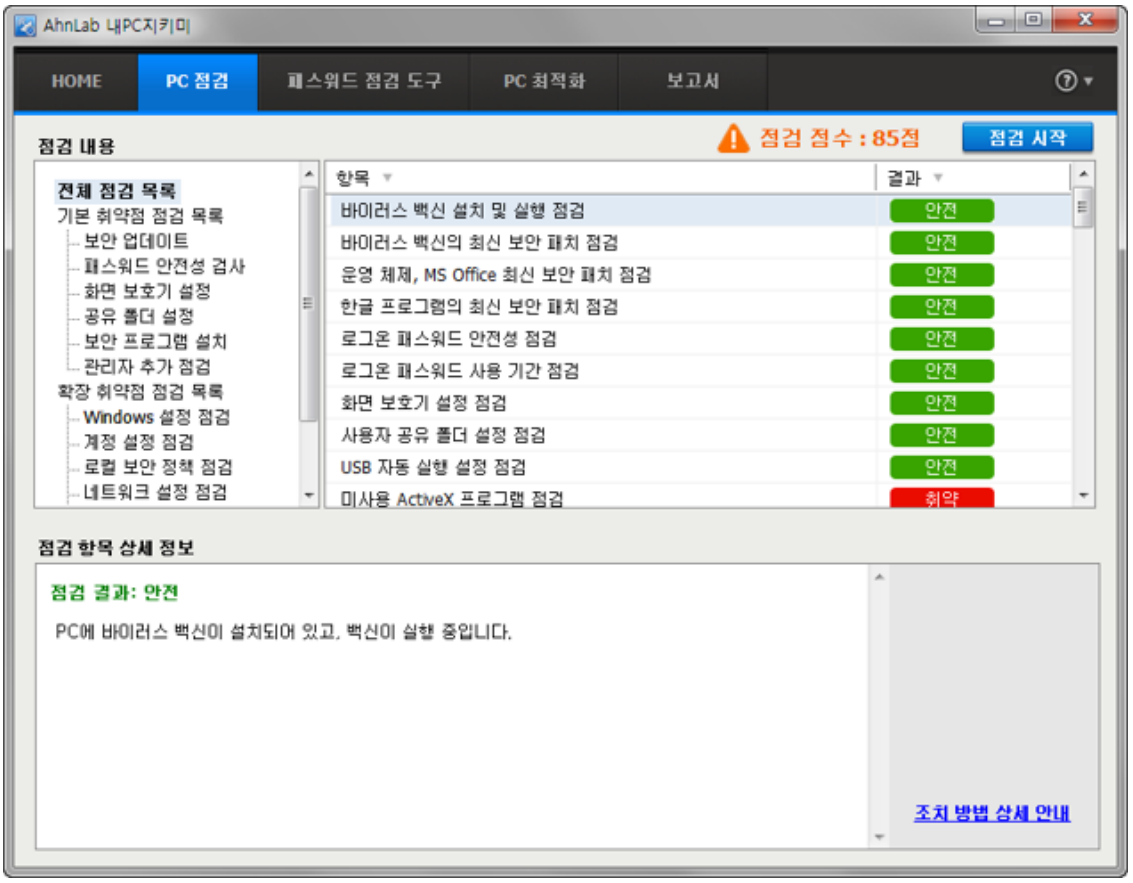
PC 점검

PC 점검에서는 기본 취약점 목록과 확장 취약점 목록에 대해 검사를 수행할 수 있습니다.

PC 점검 화면

PC 점검 화면은 다음과 같이 **점검 내용**과 각 점검 항목에 대한 **점검 항목 상세 정보**로 구성되어 있습니다.

- 점검 점수: PC 점검을 수행한 결과 점수입니다. 점검 점수에 반영되는 항목은 HOME 화면의 **PC 점검 점수 반영 항목**에서 확인할 수 있습니다.
- 점검 시작: **점검 시작** 버튼을 눌러 PC 점검을 수행할 수 있습니다.



점검 내용

점검 내용은 **기본 취약점 점검 목록**과 **확장 취약점 점검 목록**으로 나뉩니다.

- 기본 취약점 점검 목록: Windows 보안 업데이트와 로그온 패스워드 설정, 화면 보호기 설정, 공유 폴더 설정, 보안 프로그램 설치 및 관리자의 추가 점검 항목에 대해 점검합니다.
- 확장 취약점 점검 목록: Windows 설정, 계정 설정, 로컬 보안 정책 설정, 웹 브라우저 설정 및 기타 설정 항목을 점검합니다.

점검 항목 상세 정보

점검 결과에 대한 상세 설명을 나타냅니다. 점검 결과가 '취약'으로 진단된 경우, **조치 방법 상세 안내**를 눌러 조치 방법을 확인할 수 있습니다.

관리자 지정 점검

관리자가 설정한 점검 날짜와 점검 모드에 따라 사용자 PC 에 내 PC 지키미 점검을 수행합니다.

- 백그라운드 검사 후 점검 결과 화면 표시: 내 PC 지키미 검사 화면을 사용자 PC 에 표시하지 않고 검사한 후, 점검 결과만 화면에 표시합니다.
- 점검 화면 노출 없이 백그라운드로 검사: 내 PC 지키미 검사 화면을 사용자 PC 에 표시하지 않고 검사합니다. 로그온 패스워드의 안전성 점검의 경우, 이전에 입력된 로그온 패스워드가 없으면 패스워드 건너 띄기로 점검이 진행됩니다.
- 점검 화면만 노출(사용자가 직접 검사): 내 PC 지키미 검사 화면만 실행되며, 검사 진행 여부는 사용자가 직접 선택합니다.

기본 취약점 점검 목록

보안 업데이트

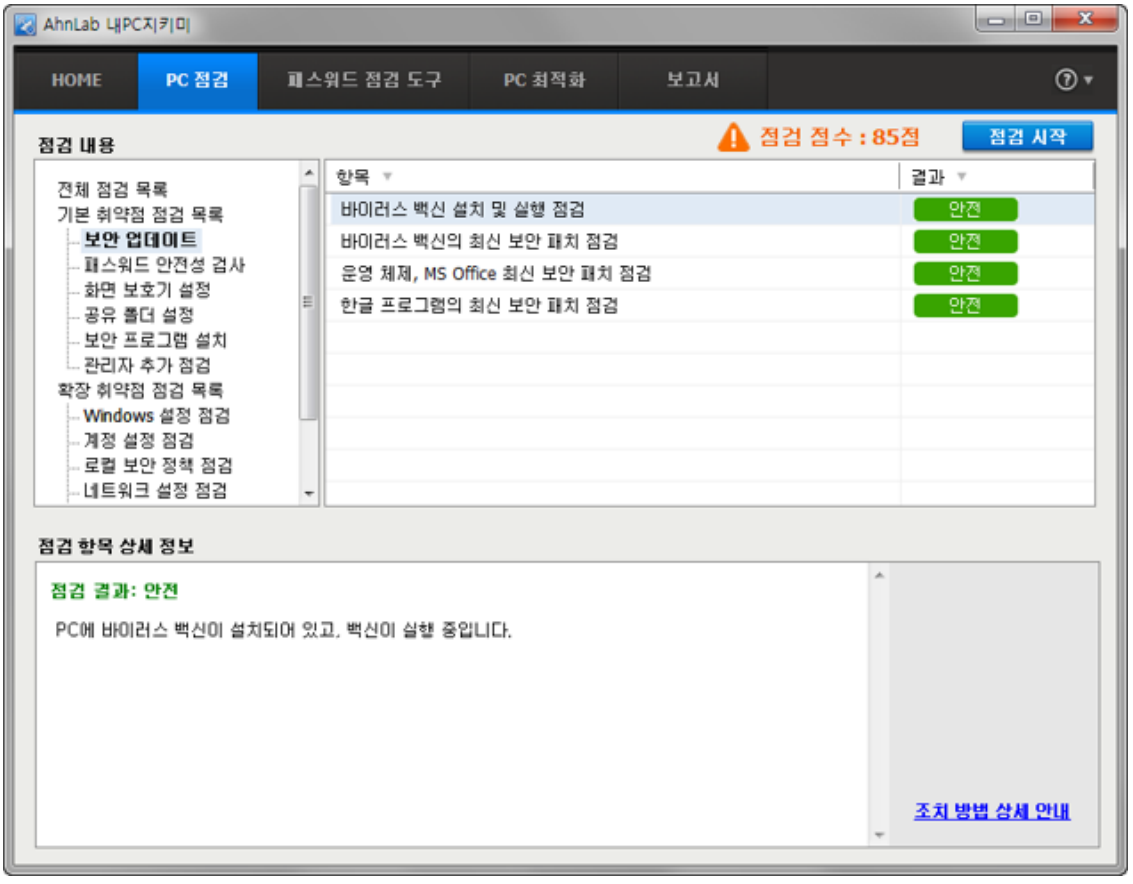
바이러스 백신 설치 및 실행 점검

바이러스 백신 설치 및 실행 점검에서는 바이러스 백신이 설치되어 있는 지 확인하고 설치된 백신의 실행 여부를 점검합니다.

점검 방법

바이러스 백신 설치 및 실행 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내PC지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > 보안 업데이트에서 바이러스 백신 설치 및 실행 점검을 선택합니다.



4. 바이러스 백신 설치 및 실행 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 바이러스 백신이 설치되어 있고 실행중인 경우입니다.
   - 취약: 바이러스 백신이 설치되지 않았거나 백신이 설치는 되어 있지만 실행이 되지 않은 경우입니다. 점검 결과가 취약인 경우에는 **백신 상태 확인하기**를 눌러 보안 센터에서 바이러스 백신의 설치 여부와 설치된 바이러스 백신의 사용 여부를 확인하십시오.

- 점검 불가: 바이러스 백신의 설치 여부를 확인할 수 없는 경우입니다.

조치 방법

- 바이러스 백신 설치 및 실행 점검

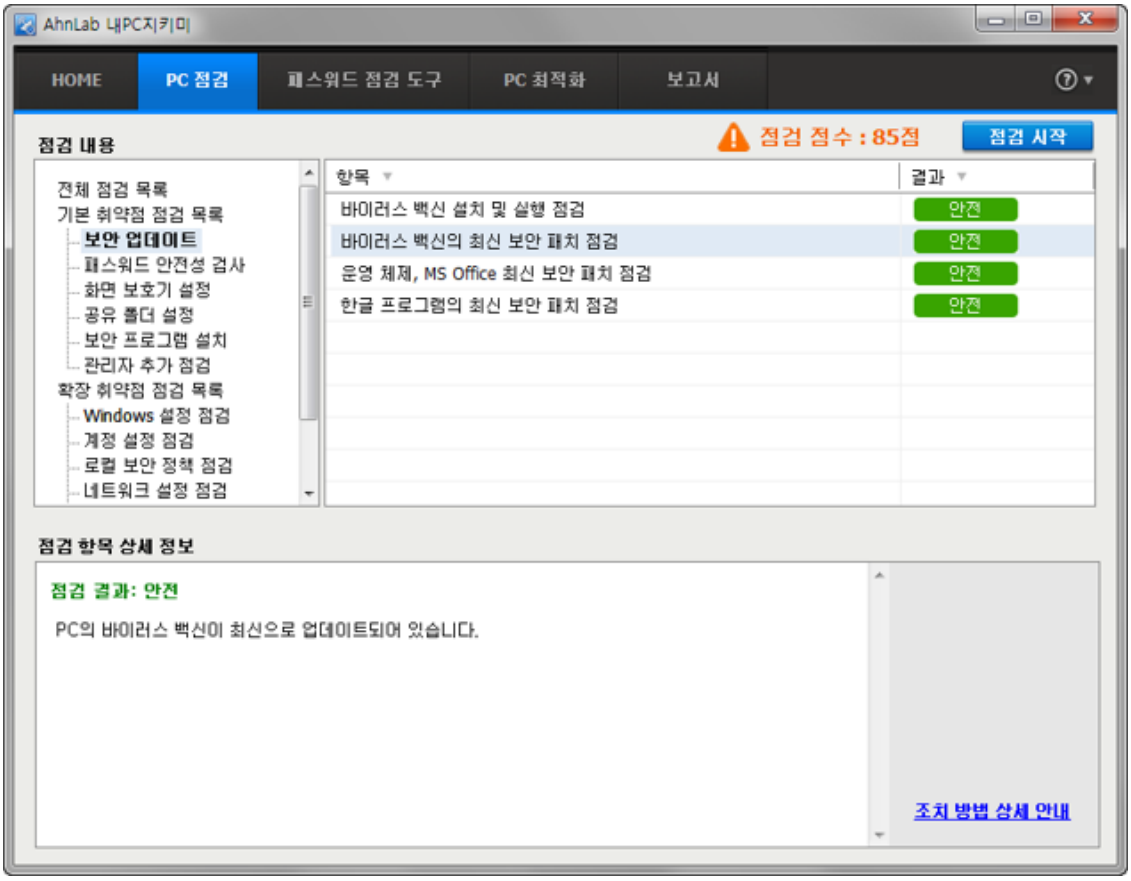
바이러스 백신의 최신 보안 패치 점검

바이러스 백신 프로그램에 최신 보안 패치가 적용되었는지 점검합니다.

점검 방법

바이러스 백신의 최신 보안 패치 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내PC지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > 보안 업데이트에서 바이러스 백신의 최신 보안 패치 점검을 선택합니다.



4. 바이러스 백신의 최신 보안 패치 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 바이러스 백신 프로그램에 최신 보안 패치가 적용되어 있는 경우입니다.
   - 취약: 바이러스 백신 프로그램에 최신 보안 패치가 적용되지 않은 경우입니다. **관리 센터 실행하기**를 눌러 보안 센터에 등록된 바이러스 백신이 최신 업데이트 상태인지 확인합니다. 바이러스 백신이 최신 업데이트 상태가 아닌 경우, **지금 업데이트**를 눌러 바이러스 백신을 업데이트합니다.
   - 점검 불가: 바이러스 백신 프로그램의 최신 보안 패치 적용 여부를 확인할 수 없는 경우입니다.

조치 방법

- 바이러스 백신의 최신 보안 패치 점검

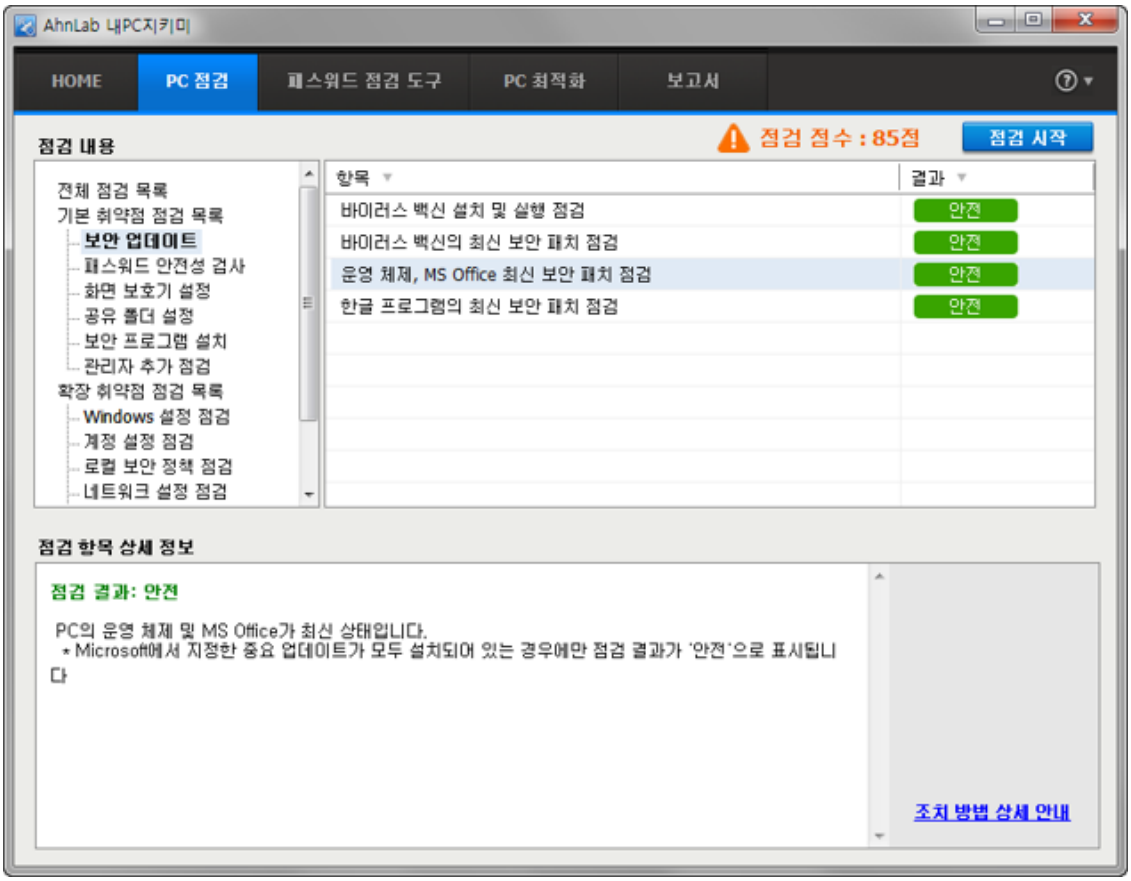
운영 체제, MS Office 최신 보안 패치 점검

Windows 운영 체제와 MS Office 프로그램의 최신 보안 패치 설치 여부를 점검합니다. 운영 체제와 MS Office 의 최신 보안 패치 점검은 Windows 업데이트 기능을 통해 사용자 PC 의 패치 설치 여부를 판단합니다.

점검 방법

운영 체제, MS Office 의 최신 보안 패치 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내PC지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > 보안 업데이트에서 운영체제, MS Office 최신 보안 패치 점검을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: Windows 운영 체제와 MS Office 프로그램에 최신 보안 패치가 적용되어 있는 경우입니다.
   - 취약: Windows 운영 체제와 MS Office 프로그램에 최신 보안 패치가 적용되지 않은 경우입니다.
   - 점검 불가: Windows 운영 체제와 MS Office 프로그램의 최신 보안 패치 적용 여부를 확인할 수 없는 경우입니다.

조치 방법

- 운영 체제, MS Office 최신 보안 패치 점검

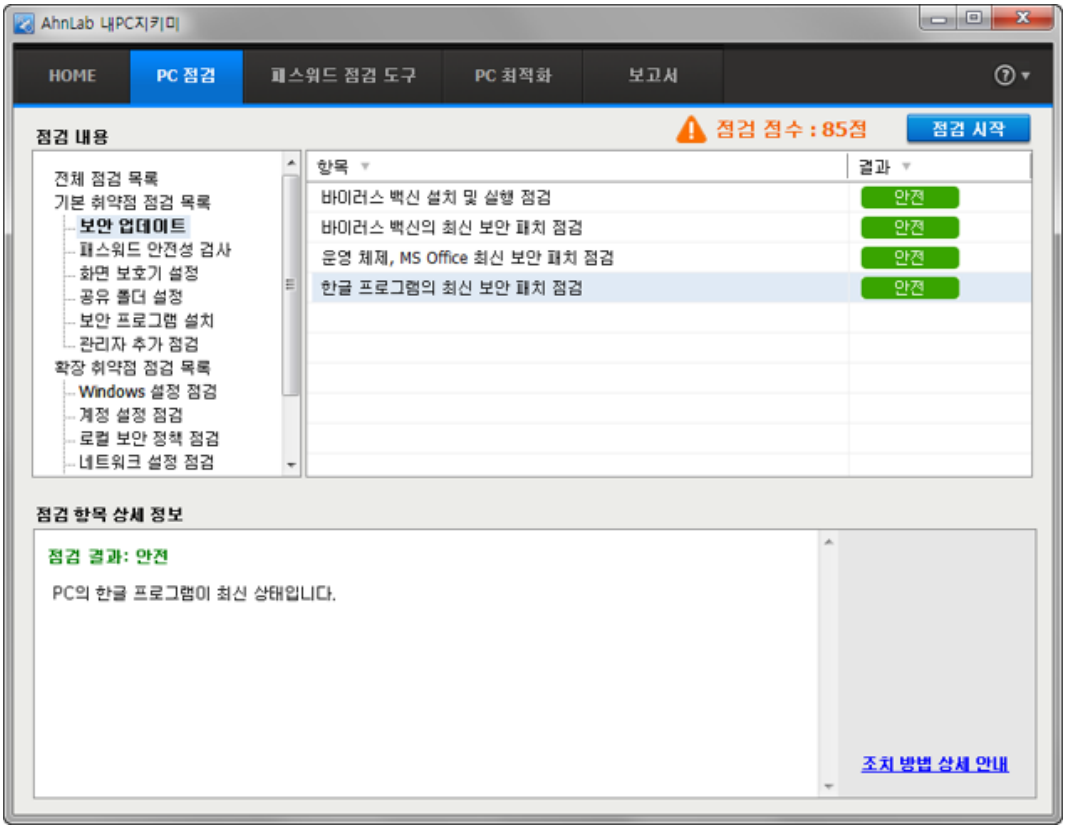
한글 프로그램의 최신 보안 패치 점검

한글 프로그램의 최신 보안 패치 적용 여부를 점검합니다. 시스템 관리자가 설정한 한글 프로그램의 최신 버전 설정 값과 사용자 PC 의 한글 프로그램 버전을 비교하거나 한글 프로그램의 최신 정보를 참고하여 자동 점검합니다.

점검 방법

한글 프로그램의 최신 보안 패치 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 기본 취약점 점검 목록 > 보안 업데이트에서 한글 프로그램의 최신 보안 패치 점검을 선택합니다.



4. 항목의 **한글프로그램의 최신 보안 패치 점검**을 선택하면 아래에 점검 항목 상세 정보가 표시됩니다.
   - 안전: 한글 프로그램에 최신 보안 패치가 적용되어 있는 경우입니다.
   - 취약: 한글 프로그램에 최신 보안 패치가 적용되지 않은 경우입니다. **업데이트 설치하기**를 눌러 최신 보안 패치를 적용하십시오.
   - 점검 불가: 한글 프로그램의 최신 보안 패치 적용 여부를 확인할 수 없는 경우입니다.

참고

한컴 자동 업데이트 프로그램에서 최신 버전으로 표시되고 있으나 내 PC 지키미 점검 결과가 **취약**으로 판정되는 경우, 한글과 컴퓨터 홈페이지에서 최신 업데이트를 직접 다운로드 하여 설치하십시오.

조치 방법

- 한글 프로그램의 최신 보안 패치 점검

패스워드 안전성 검사

로그온 패스워드 안전성 점검

내 PC 지키미 검사를 실행할 때 입력한 Windows 로그온 패스워드에 대해 다음의 점검 항목을 기준으로 안전성을 점검합니다.

점검 항목

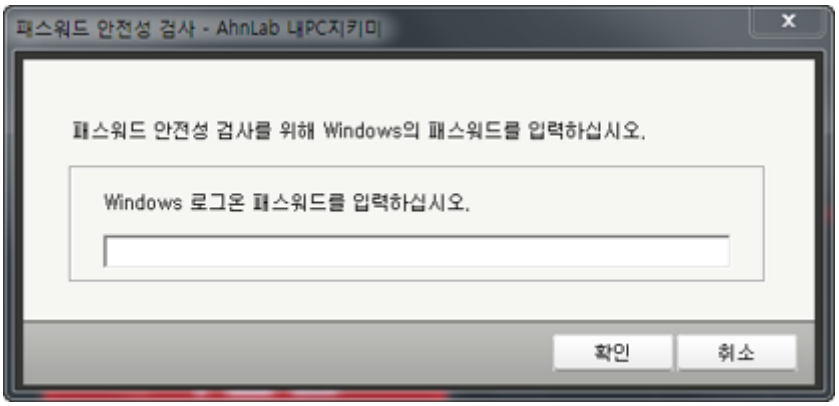
- Windows 로그온 패스워드 사용 점검
- 사용자 계정과 동일한 패스워드 사용 점검
- 로그온 패스워드의 길이 및 필수문자 조합이 안전 조건을 준수하는지 점검

참고
패스워드 안전성 검사 화면은 내 PC 지키미 검사를 최초 실행하거나 패스워드를 변경했을 경우 확인할 수 있습니다.

점검 방법

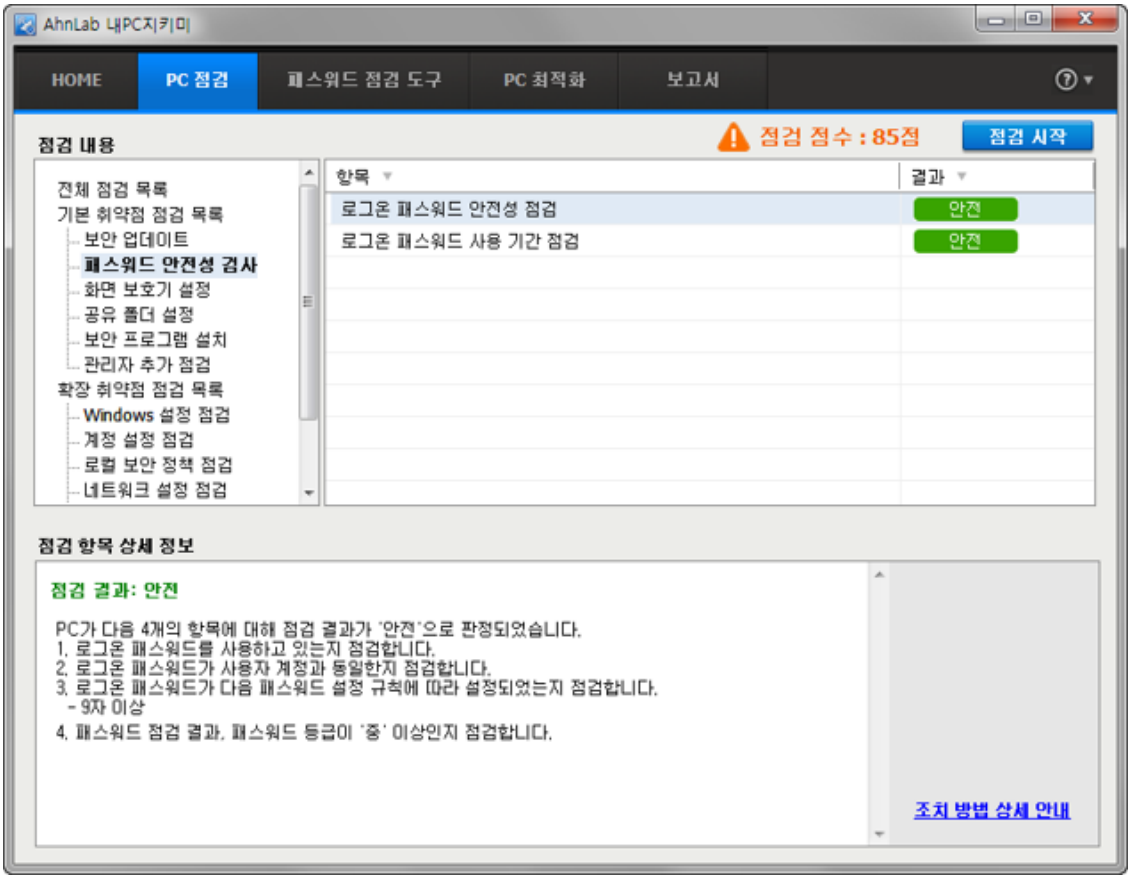
로그온 패스워드 안정성 점검 방법은 다음과 같습니다.

1. 내PC지키미를 실행한 후 패스워드 안전성 검사에서 Windows 로그온 패스워드를 입력합니다.



참고
패스워드 안전성 검사를 실패했을 경우에는 **패스워드 검사 건너뛰기**를 선택하면 로그온 패스워드 안전성 점검을 수행하지 않으며 점검 결과는 **취약**으로 표시됩니다.

2. 보안 점검을 실행하여 점검 결과를 확인합니다.
3. 점검 완료 창을 닫은 후 내PC지키미의 **PC 점검** 탭을 선택합니다.
4. 점검 내용의 기본 취약점 점검 목록 > **패스워드 안전성 검사**에서 로그온 패스워드 안전성 점검을 선택합니다.



5. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
    - 안전: 패스워드 안전성 점검 항목을 모두 만족하는 경우입니다.
    - 취약: 패스워드 안전성 점검 항목 중 한 가지 항목이라도 위반되는 경우가 있는 경우입니다.
    - 점검 불가: 패스워드를 입력하지 않았거나 기타 사유로 로그온 패스워드 안전성을 확인할 수 없는 경우입니다.

조치 방법

- 로그온 패스워드 안전성 점검

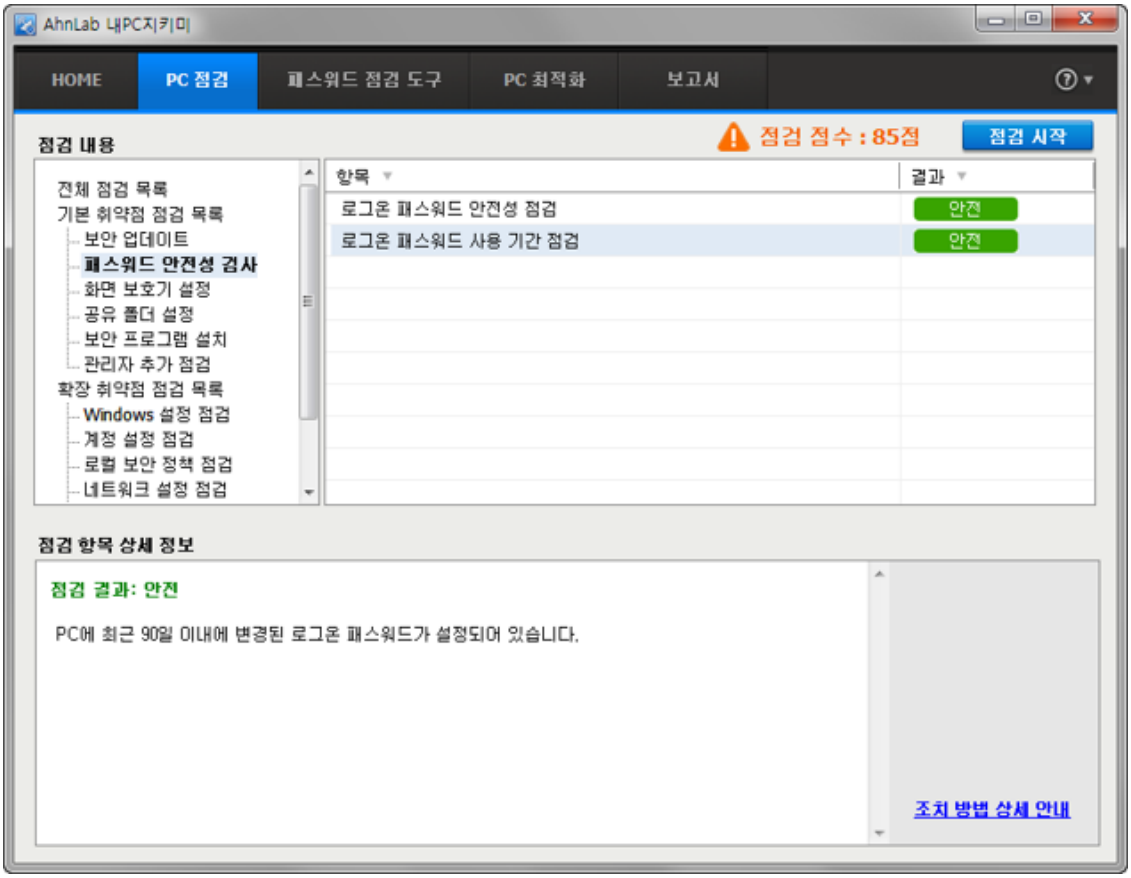
로그온 패스워드 사용 기간 점검

관리자가 설정한 Windows 로그온 패스워드의 사용 기간이 지났는지 점검합니다.

점검 방법

로그온 패스워드 사용 기간 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내PC지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > **패스워드 안전성 검사**에서 로그온 패스워드 사용 기간 점검을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 로그온 패스워드 변경일로부터 관리자가 설정한 기간이 경과하지 않은 경우입니다.
   - 취약: 로그온 패스워드 변경일로부터 관리자가 설정한 기간이 지난 경우입니다. 취약한 패스워드로 진단된 경우에는 **패스워드 변경**을 눌러 현재 사용 중인 패스워드를 변경하시기 바랍니다.

조치 방법

- 로그온 패스워드 사용 기간 점검

화면 보호기 설정

화면 보호기 설정 점검

화면 보호기 설정에서는 사용자 PC 의 화면 보호기 사용 여부와 대기 시간, 패스워드 설정 여부를 확인하여 안전성을 점검합니다.

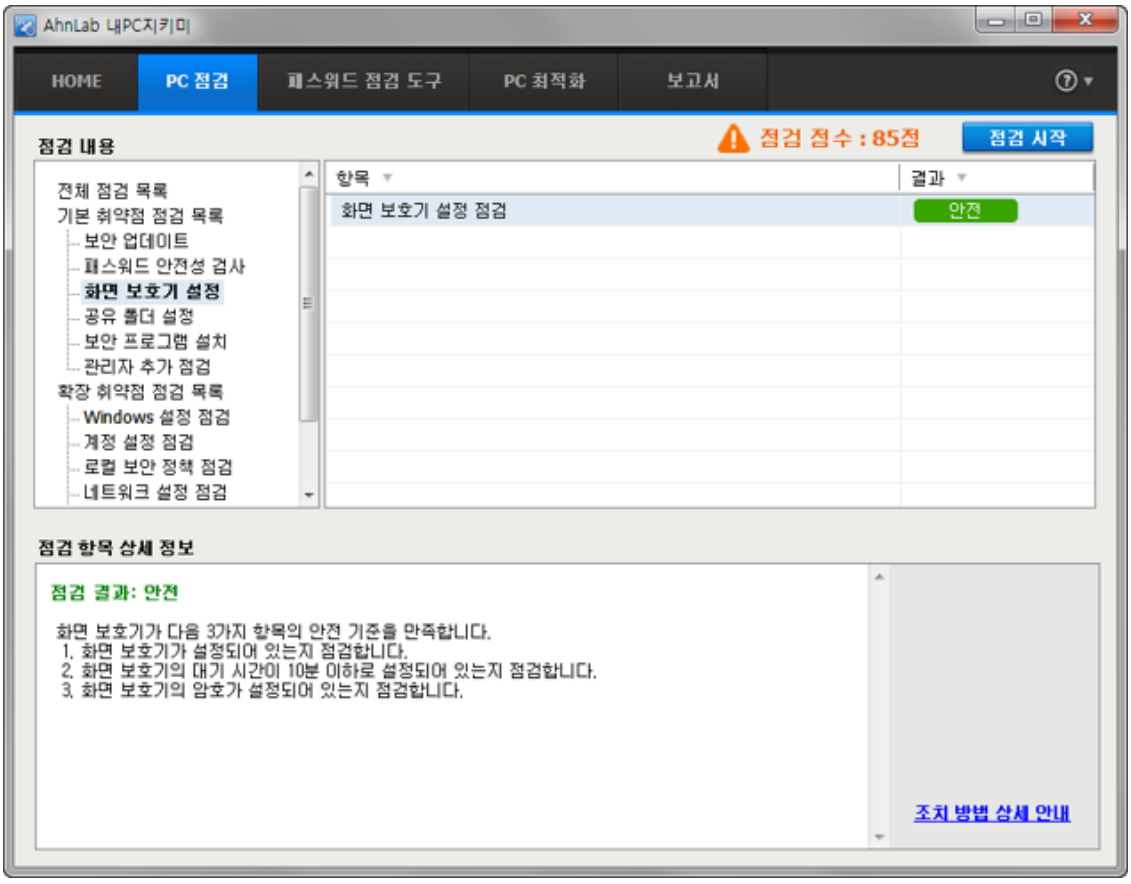
화면 보호기 안전 조건

- 화면 보호기 **사용**이 선택이 되어 있는지 점검합니다.
- 화면 보호기 대기 시간이 관리자가 설정한 시간 이내로 설정되어 있는 지 점검합니다.
- 화면 보호기 해제를 위한 로그온 화면 표시를 사용하고 있는지 점검합니다.

점검 방법

화면 보호기 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > **화면 보호기 설정**에서 **화면 보호기 설정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
    - 안전: 화면 보호기가 설정되어 있고, 대기 시간이 관리자가 설정한 시간 이내이며 화면 보호기 해제 시에 패스워드가 설정되어 있는 경우입니다.

- 취약: 화면 보호기가 설정되어 있지 않거나, 대기 시간이 관리자가 지정한 설정 값 이상이거나, 화면 보호기 해제 시에 패스워드가 설정되어 있지 않은 경우입니다. 점검 결과가 취약인 경우에는 **화면 보호기 설정**을 눌러 화면 보호기를 설정하시기 바랍니다.
- 점검 불가: 화면 보호기 설정 여부를 확인할 수 없는 경우입니다.

조치 방법

- 화면 보호기 설정 점검

공유 폴더 설정

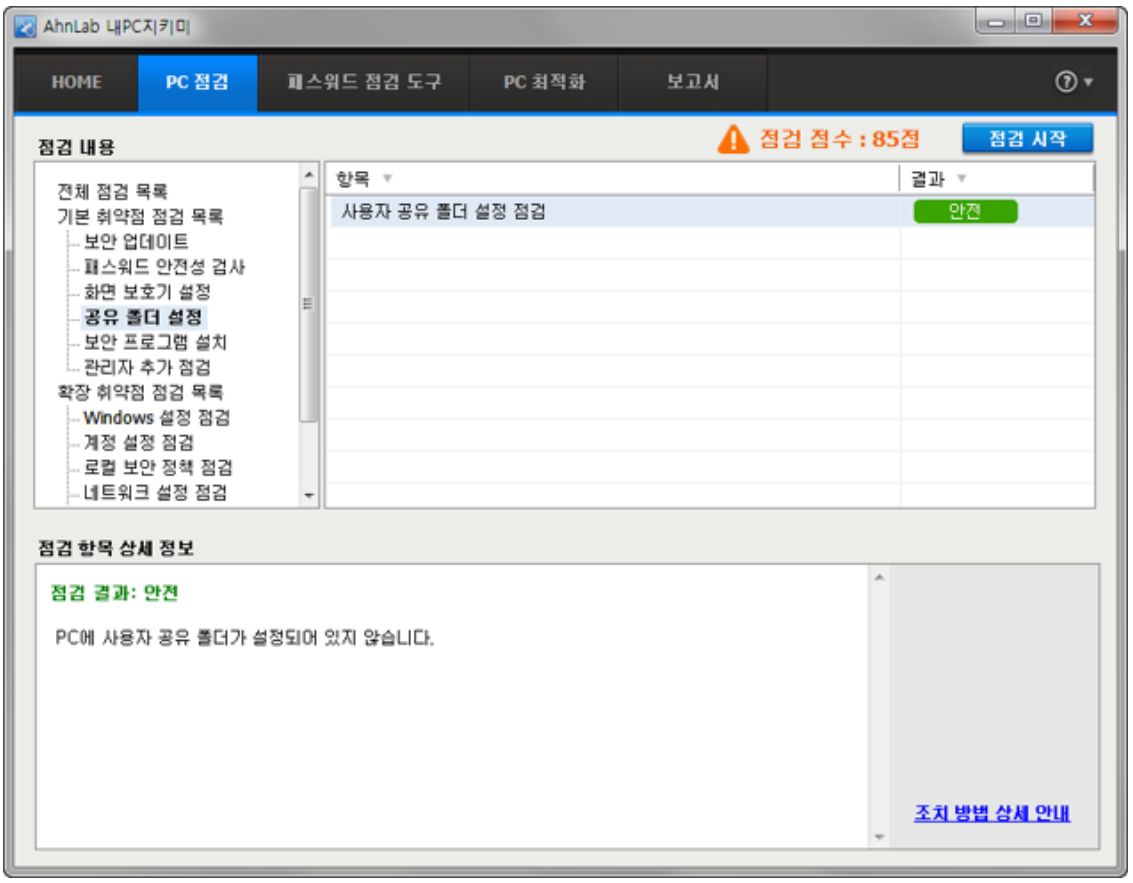
사용자 공유 폴더 설정 점검

사용자 공유 폴더 설정 점검에서는 사용자 PC 에 설정되어 있는 공유 폴더를 점검합니다.

점검 방법

사용자 공유 폴더 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > 공유 폴더 설정에서 **사용자 공유 폴더 설정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 사용자 공유 폴더가 설정되어 있지 않은 경우입니다.
   - 취약: 사용자 공유 폴더가 설정되어 있는 경우입니다. 점검 결과가 취약인 경우에는 **공유 폴더 해제하기**를 눌러 설정된 공유 폴더를 해제하시기 바랍니다.
   - 점검 불가: 사용자 공유 폴더 설정 여부를 확인할 수 없는 경우입니다. 점검 불가 사유에 대해서는 점검 항목 상세 정보에 표시됩니다.

조치 방법

- 사용자 공유 폴더 설정 점검

보안 프로그램 설치

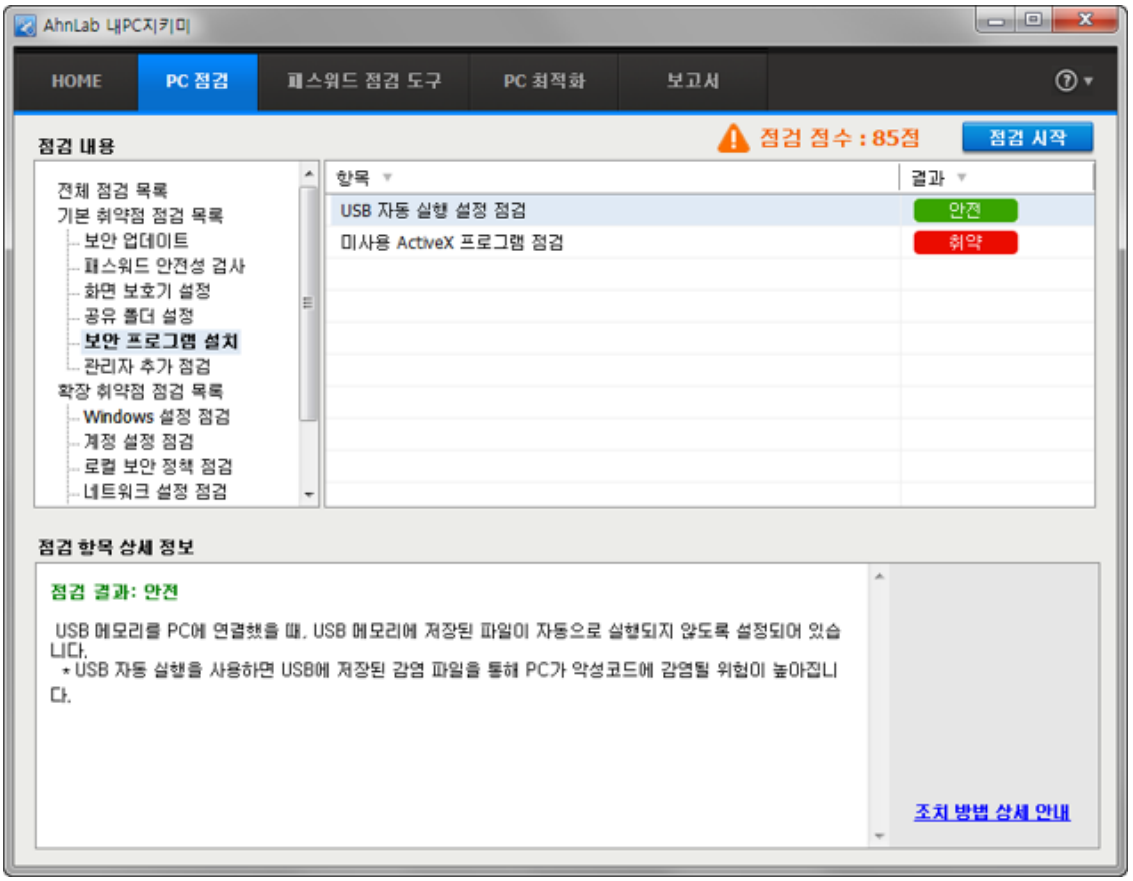
USB 자동 실행 설정 점검

USB 자동 실행 설정 점검에서는 사용자 PC 에 USB 가 연결되었을 때 자동으로 실행되도록 설정되어 있는지 점검합니다.

점검 방법

USB 자동 실행 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > 보안 프로그램 설치에서 USB 자동 실행 설정 점검을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: USB 자동 실행이 허용되지 않은 경우입니다.
   - 취약: USB 자동 실행이 허용된 경우입니다. 취약으로 진단된 경우, **USB 자동 실행 차단하기**를 눌러 USB 자동 실행이 허용되지 않도록 설정해야 합니다.

조치 방법

- USB 자동 실행 설정 점검

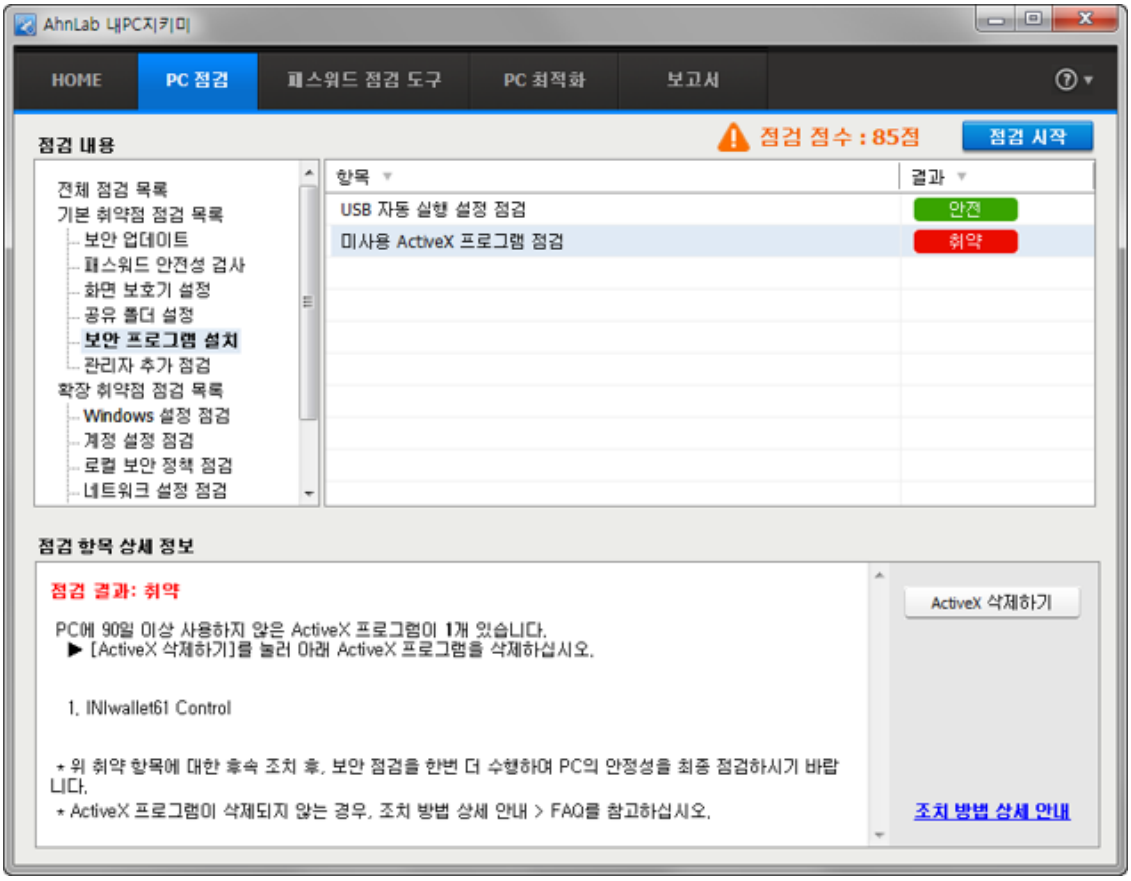
미사용 ActiveX 프로그램 점검

미사용 ActiveX 프로그램 점검에서는 관리자가 설정한 기간이 지나도록 사용하지 않은 ActiveX 프로그램이 있는지 점검합니다.

점검 방법

미사용 ActiveX 프로그램 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > 보안 프로그램 설치에서 미사용 ActiveX 프로그램 점검을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 관리자가 설정한 기간 이상 사용하지 않은 ActiveX 프로그램이 설치되어 있지 않습니다.
   - 취약: 관리자가 설정한 기간 이상 사용하지 않은 ActiveX 프로그램이 설치되어 있는 경우입니다. 취약으로 진단된 경우, **ActiveX 삭제하기**를 눌러 ActiveX 프로그램 목록에서 관리자가 설정한 기간 이상 사용하지 않은 ActiveX 프로그램을 삭제해야 합니다.

조치 방법

- 미사용 ActiveX 프로그램 점검

관리자 추가 점검

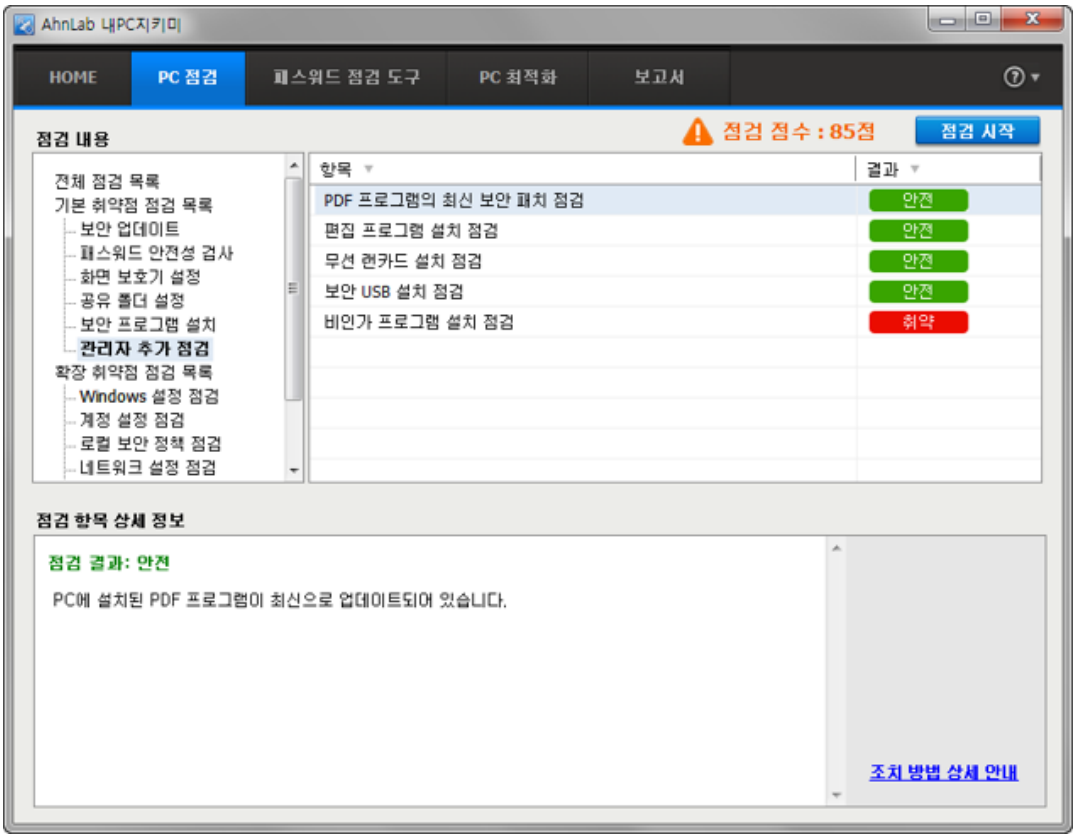
PDF 프로그램의 최신 보안 패치 점검

Adobe PDF 프로그램의 최신 버전 정보와 사용자 PC 에 설치된 PDF 프로그램의 버전 정보를 비교하여 최신 보안 패치 적용 여부를 점검합니다.

점검 방법

PDF 프로그램의 최신 보안 패치 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 기본 취약점 점검 목록 > 관리자 추가 점검에서 **PDF 프로그램의 최신 보안 패치 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: PDF 프로그램의 최신 보안 패치가 적용되어 있는 경우입니다.
   - 취약: PDF 프로그램의 최신 보안 패치가 적용되지 않은 경우입니다. 취약으로 진단된 경우에는 **[업데이트 설치하기]**를 눌러 Adobe 홈페이지에서 PDF 프로그램의 최신 보안 패치를 다운로드 하여 업데이트를 진행하십시오.
   - 점검 불가: PDF 프로그램의 최신 보안 패치가 적용 여부를 확인할 수 없는 경우입니다. 점검 불가 사유에 대해서는 점검 항목 상세 정보에 표시됩니다.

조치 방법

- PDF 프로그램의 최신 보안 패치 점검

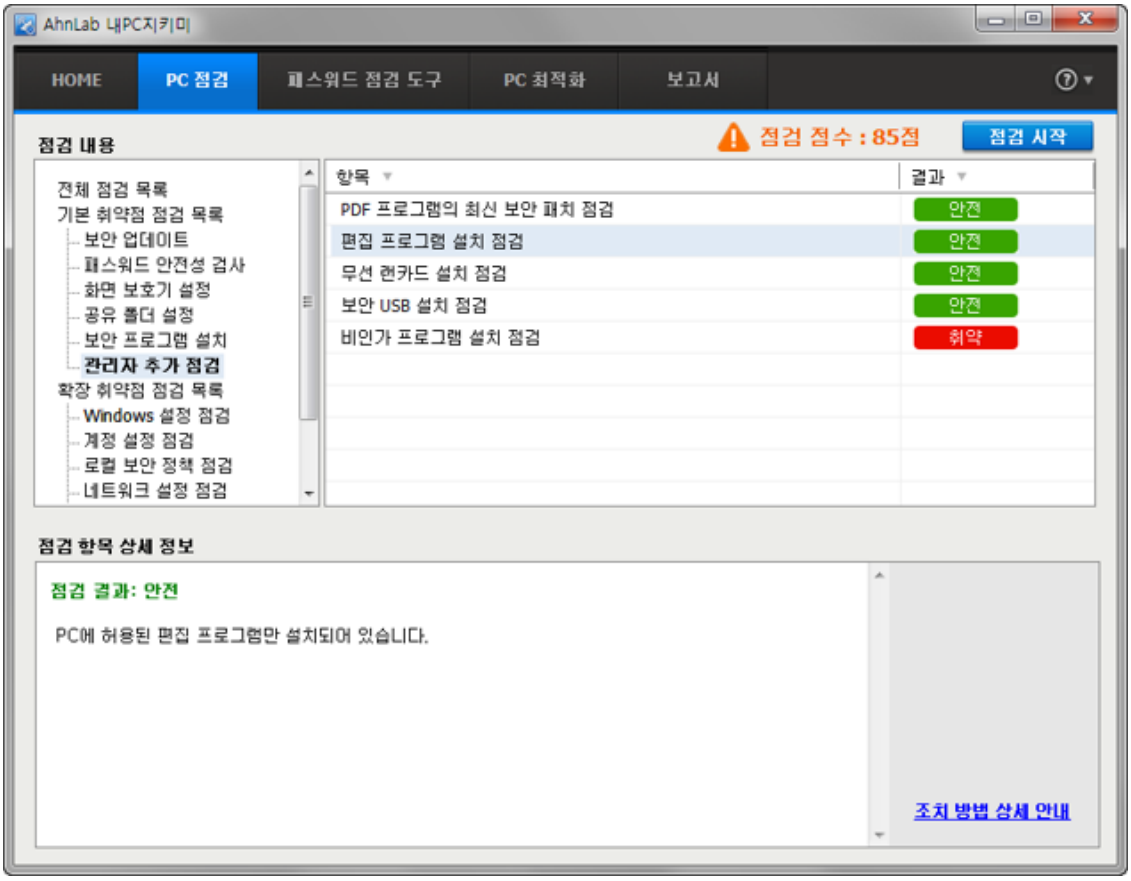
편집 프로그램 설치 점검

라이선스 권한이 없는 편집 프로그램(MS 워드, 한글 프로그램, Adobe PDF 프로그램)이 설치되었는지 확인하고 설치된 프로그램이 있는 경우 점검 결과를 취약으로 표시합니다. 취약으로 표시된 경우에는 설치된 편집 프로그램을 삭제해야 합니다.

점검 방법

편집 프로그램 설치 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > 관리자 추가 점검에서 **편집 프로그램 설치 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 점검 대상 편집 프로그램이 설치되어 있지 않은 경우입니다.
   - 취약: 점검 대상 편집 프로그램이 설치되어 있는 경우입니다. 취약으로 진단된 경우 설치된 편집 프로그램의 이름을 확인하고 **프로그램 삭제하기**를 눌러 해당 프로그램을 모두 삭제하십시오.
   - 점검 불가: 점검 대상 편집 프로그램의 설치 여부를 확인할 수 없는 경우입니다. 점검 불가 사유에 대해서는 점검 항목 상세 정보에 표시됩니다.

조치 방법

- 편집 프로그램 설치 점검

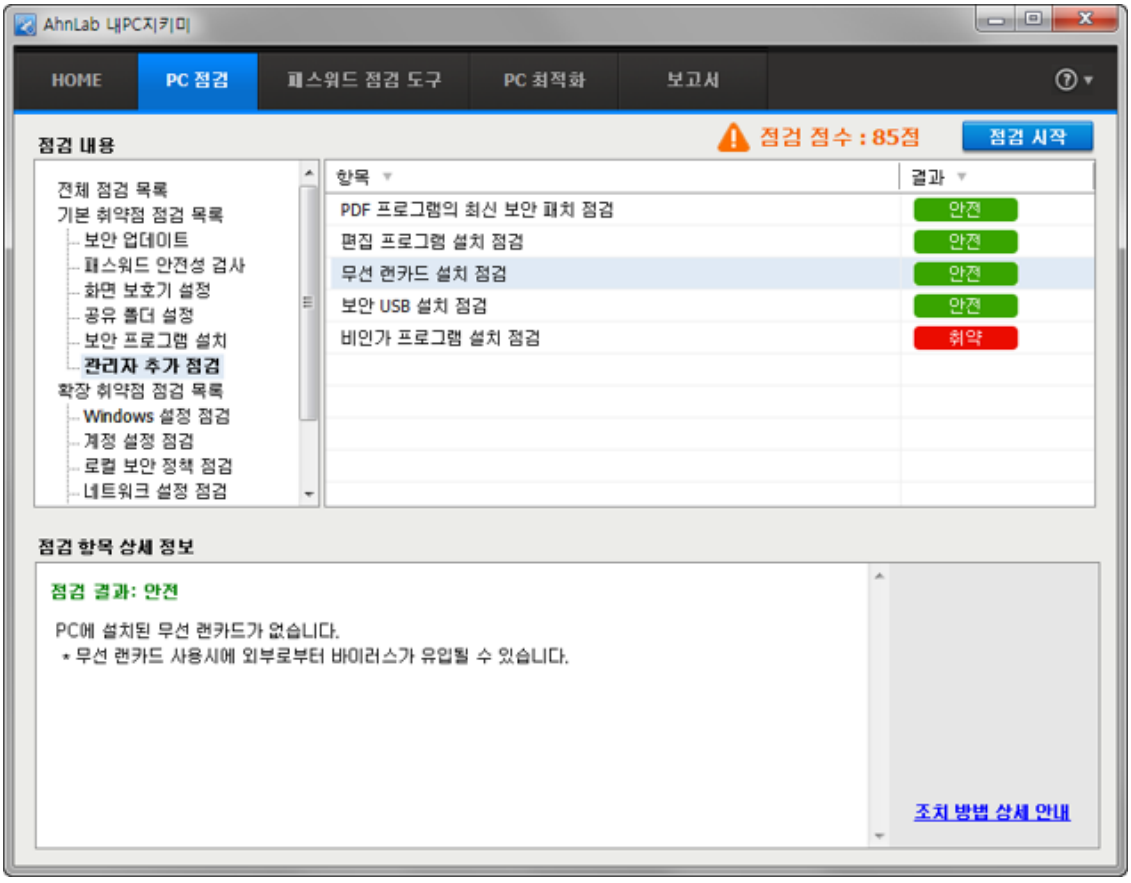
무선 랜카드 설치 점검

무선 랜카드가 설치되어 있는지 점검합니다. 노트북에 설치되어 있는 무선 랜카드는 무조건 취약으로 검출됩니다.

점검 방법

무선 랜카드 설치 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > 관리자 추가 점검에서 **무선 랜카드 설치 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 사용자 PC 에 무선 랜카드가 설치되어 있지 않습니다.
   - 취약: 사용자 PC 에 무선 랜카드가 설치되어 있습니다. **원클릭 조치**를 눌러 설치된 무선 랜카드를 제거하십시오.
   - 점검 불가: 사용자 PC 의 무선 랜카드 설치 여부를 확인할 수 없는 경우입니다. 점검 불가 사유에 대해서는 점검 항목 상세 정보에 표시됩니다.

조치 방법

- 무선 랜카드 설치 점검

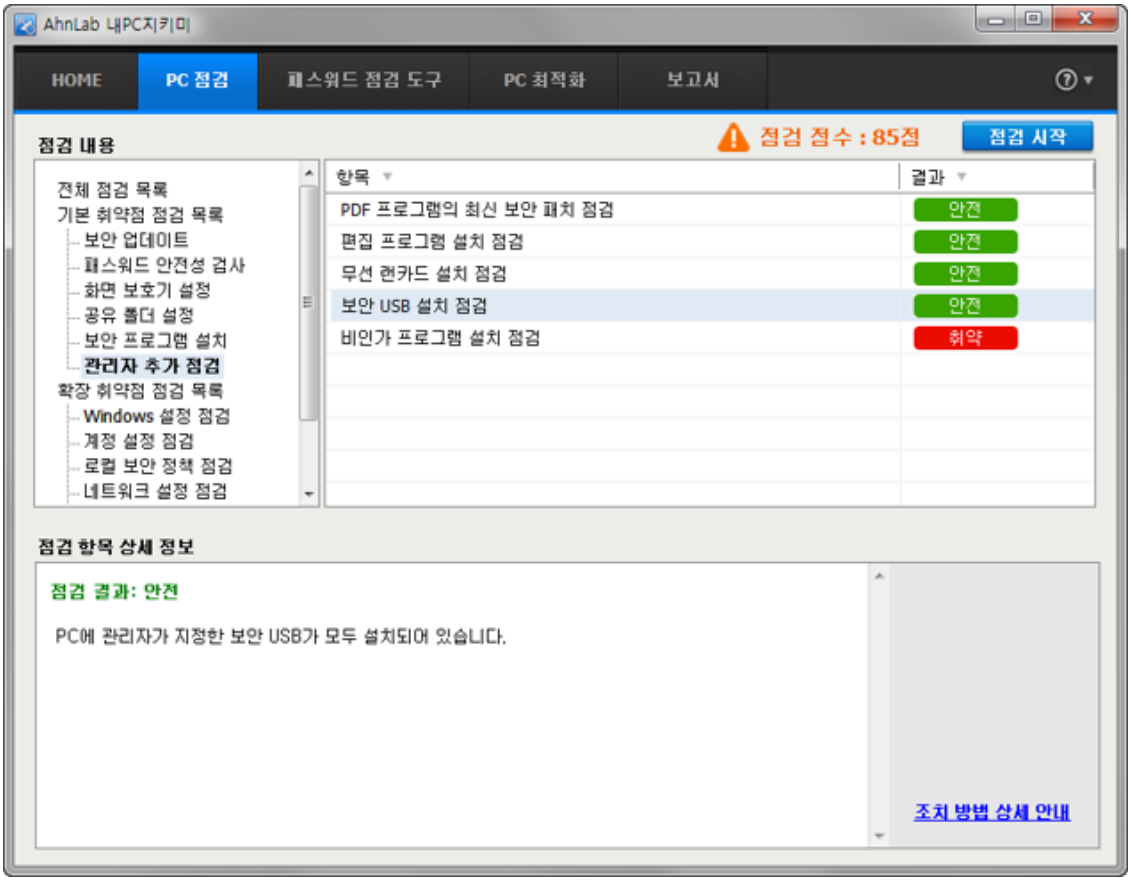
보안 USB 설치 점검

관리자가 설정한 보안 USB 의 설치 정보를 점검합니다.

점검 방법

보안 USB 설치 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > 관리자 추가 점검에서 **보안 USB 설치 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 관리자가 설정한 보안 USB 가 에이전트 PC 에 설치되어 있는 경우입니다.
   - 취약: 관리자가 설정한 보안 USB 가 에이전트 PC 에 설치되어 있지 않은 경우입니다.
   - 점검 불가: 보안 USB 설치 여부를 확인할 수 없는 경우입니다. 점검 불가 사유에 대해서는 점검 항목 상세 정보에 표시됩니다.

조치 방법

- 보안 USB 설치 점검

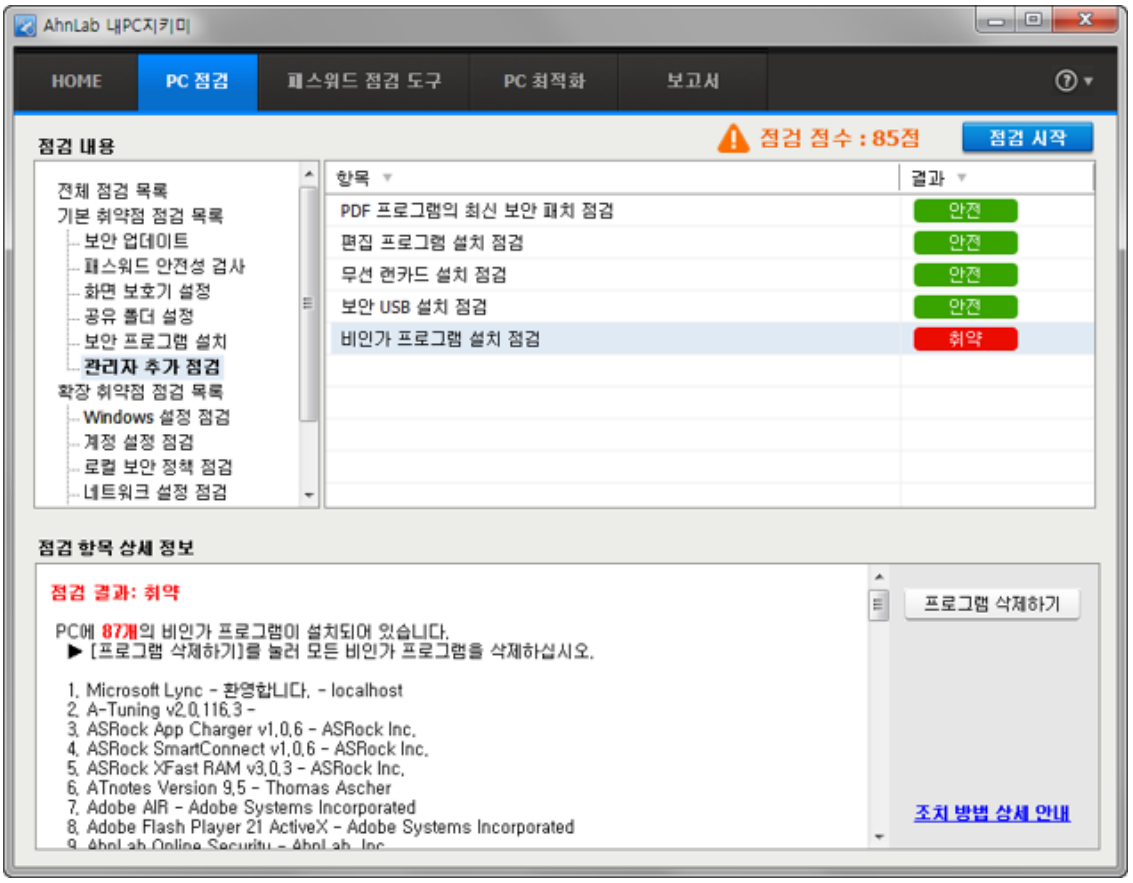
비인가 프로그램 설치 점검

관리자가 비인가 프로그램으로 등록한 프로그램이 사용자 PC 에 설치되어 있는지 점검합니다.

점검 방법

비인가 프로그램 설치 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내PC지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 기본 취약점 점검 목록 > 관리자 추가 점검에서 **비인가 프로그램 설치 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 비인가 프로그램이 사용자 PC 에 설치되어 있지 않습니다.
   - 취약: 비인가 프로그램이 사용자 PC 에 설치되어 있는 경우로 설치된 비인가 프로그램의 개수와 설치된 프로그램 목록을 보여줍니다. 취약으로 진단된 경우 설치된 비인가 프로그램의 이름을 확인하고 **프로그램 삭제하기**를 눌러 해당 프로그램을 모두 삭제하십시오.

조치 방법

- 비인가 프로그램 설치 점검

확장 취약점 점검 목록

Windows 설정 점검

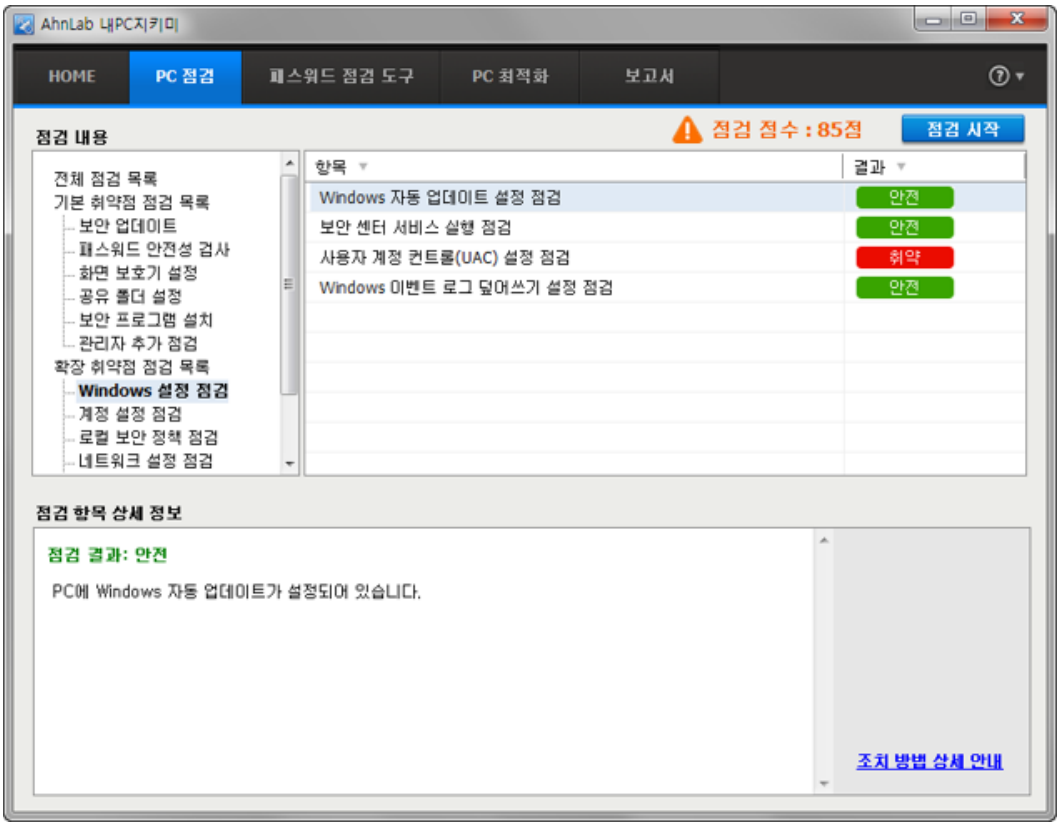
Windows 자동 업데이트 설정 점검

사용자 PC 에 Windows 자동 업데이트가 설정되어 있고, 자동으로 패치를 다운로드 하여 업데이트하는지 점검합니다.

점검 방법

Windows 자동 업데이트 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > Windows 설정 점검에서 **Windows 자동 업데이트 설정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: Windows 자동 업데이트가 설정되어 있는 경우입니다.
   - 취약: Windows 자동 업데이트가 설정되어 있지 않은 경우입니다. **원클릭 조치**를 눌러 Windows 자동 업데이트를 설정하십시오.

조치 방법

- Windows 자동 업데이트 설정 점검

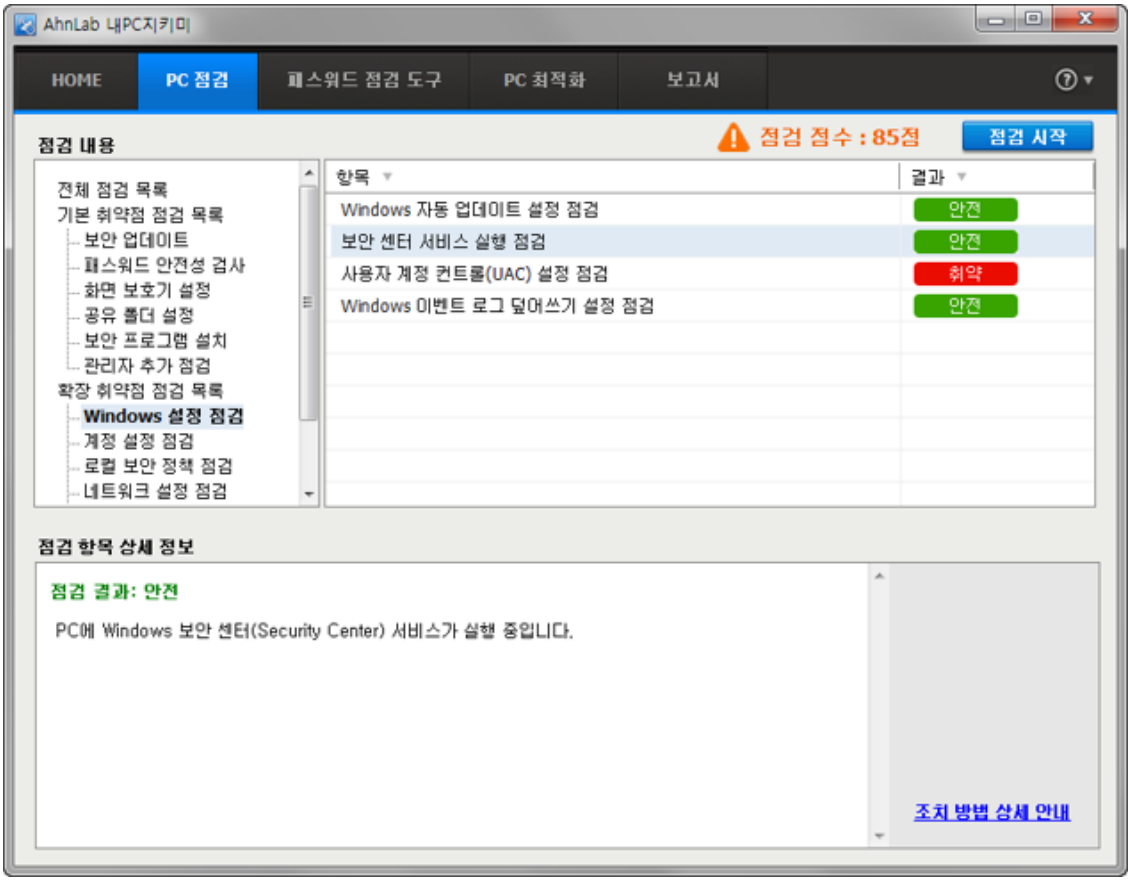
보안 센터 서비스 실행 점검

사용자 PC 에 보안 센터 서비스가 실행 중인지 점검합니다.

점검 방법

보안 센터 서비스 실행 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > Windows 설정 점검에서 **보안 센터 서비스 실행 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 보안 센터 서비스가 실행 중인 경우입니다.
   - 취약: 보안 센터 서비스가 실행 중이지 않은 경우입니다. 취약으로 진단된 경우 **서비스 실행하기**를 눌러 보안 센터 서비스를 시작하십시오.

조치 방법

- 보안 센터 서비스 실행 점검

사용자 계정 컨트롤(UAC) 사용 점검

사용자 PC 에 사용자 계정 컨트롤(UAC)이 설정되어 있는지 점검합니다.

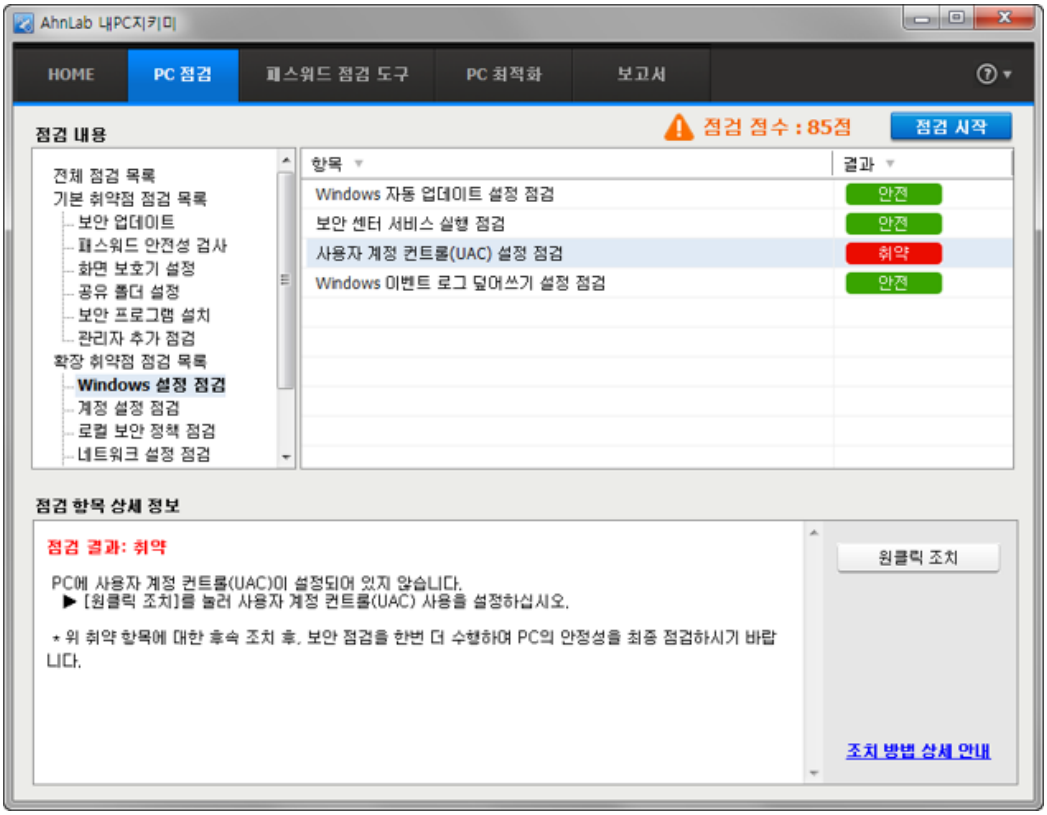
사용자 계정 컨트롤(UAC) 설정

사용자 계정 컨트롤(UAC)는 사용자 컴퓨터에서 변경 내용의 적용을 위해, 관리자 권한이 필요한 경우 이를 사용자에게 알려 줍니다. 기본 UAC 설정에서는 프로그램이 컴퓨터의 변경을 시도할 때마다 이를 사용자에게 알리지만 UAC 가 알리는 빈도를 변경할 수 있습니다. UAC 는 항상 알림, 프로그램에서 컴퓨터를 변경하려는 경우에만 알림, 프로그램에서 컴퓨터를 변경하려는 경우에만 알림, 알리지 않음의 4 가지의 설정이 있으며, 각 설정에 따라 사용자 PC 보안에 미칠 수 있는 영향이 다르게 설정됩니다.

점검 방법

사용자 계정 컨트롤(UAC) 사용 여부를 점검하는 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 확장 취약점 점검 목록 > Windows 설정 점검에서 **사용자 계정 컨트롤(UAC) 설정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 사용자 계정 컨트롤(UAC)를 사용하도록 설정되어 있습니다.
   - 취약: 사용자 계정 컨트롤(UAC)를 사용하도록 설정되어 있지 않은 경우입니다. **원클릭 조치**를 눌러 사용자 계정 컨트롤(UAC) 사용을 설정하십시오.

조치 방법

- 사용자 계정 컨트롤(UAC) 설정 점검

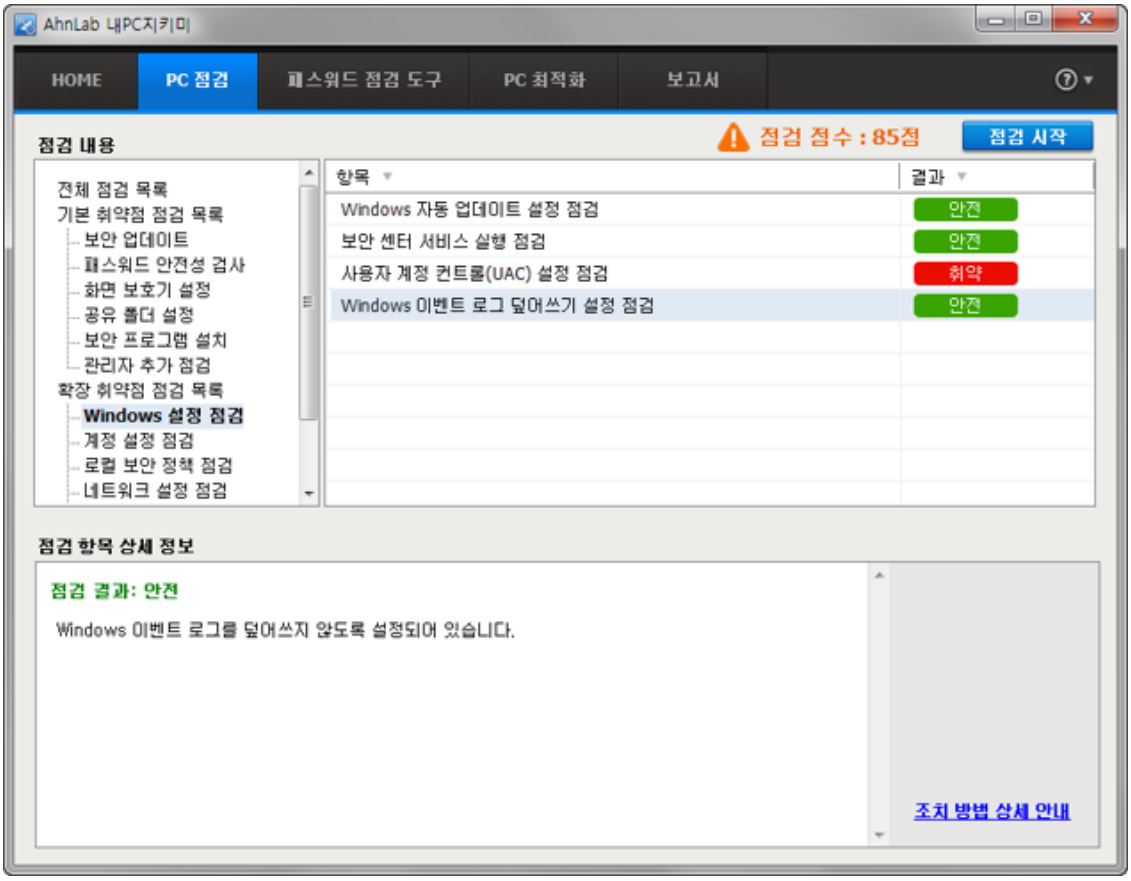
Windows 이벤트 로그 덮어쓰기 설정 점검

사용자 PC 에 Windows 이벤트 로그가 덮어쓰도록 설정되어 있는지 점검합니다.

점검 방법

Windows 이벤트 로그 덮어쓰기 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > Windows 설정 점검에서 Windows 이벤트 로그 덮어쓰기 설정 점검을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: Windows 이벤트 로그를 덮어쓰지 않도록 설정되어 있는 경우입니다.
   - 취약: Windows 이벤트 로그를 덮어쓰도록 설정되어 있는 경우입니다. 취약으로 진단된 경우, **원클릭 조치**를 눌러 Windows 이벤트 로그를 덮어쓰지 않도록 설정을 변경하십시오.

조치 방법

- Windows 이벤트 로그 덮어쓰기 설정 점검

계정 설정 점검

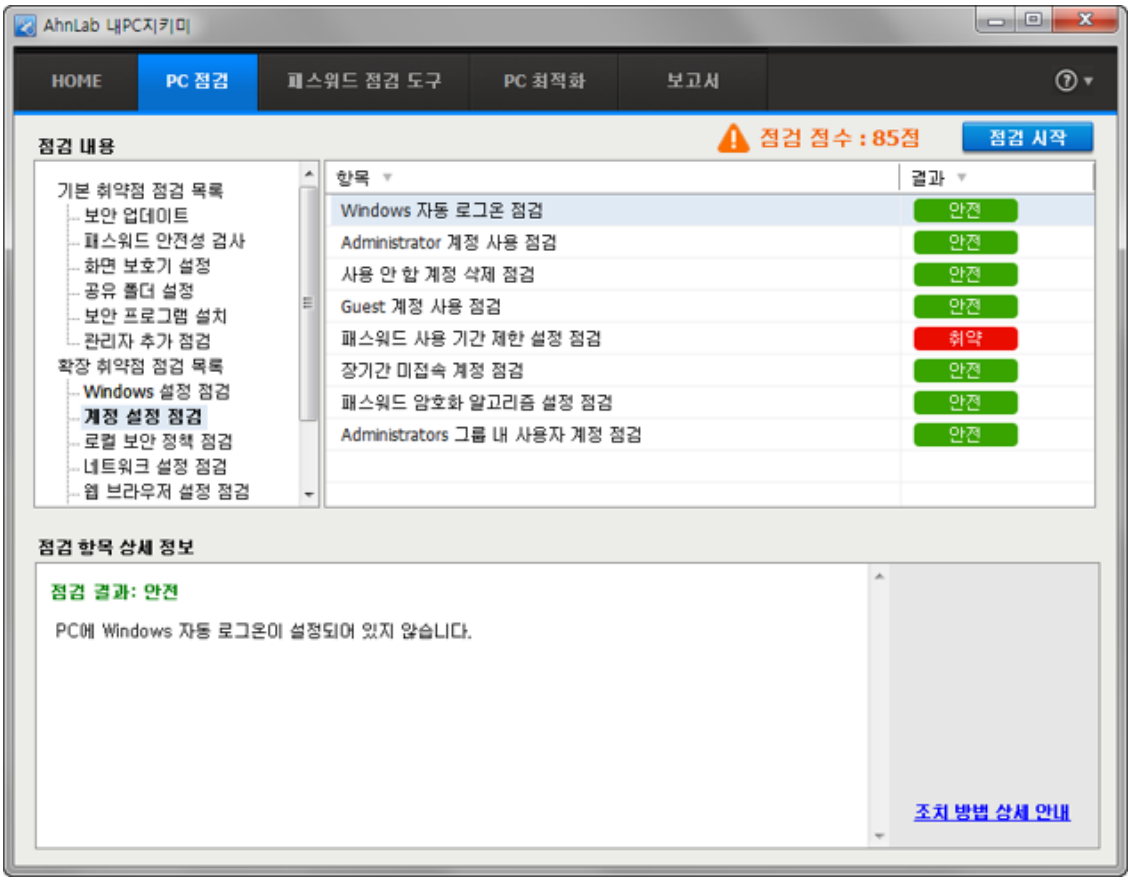
Windows 자동 로그온 점검

사용자 PC 에 Windows 자동 로그온 기능이 설정되어 있는지 점검합니다.

점검 방법

Windows 자동 로그온 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 계정 설정 점검에서 **Windows 자동 로그온 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: Windows 자동 로그온이 설정되어 있지 않은 경우입니다.
   - 취약: Windows 자동 로그온이 설정되어 있는 경우입니다. 취약으로 진단된 경우, **자동 로그온 해제** 버튼을 눌러 Windows 자동 로그온 설정을 해제하십시오.

조치 방법

- Windows 자동 로그온 점검

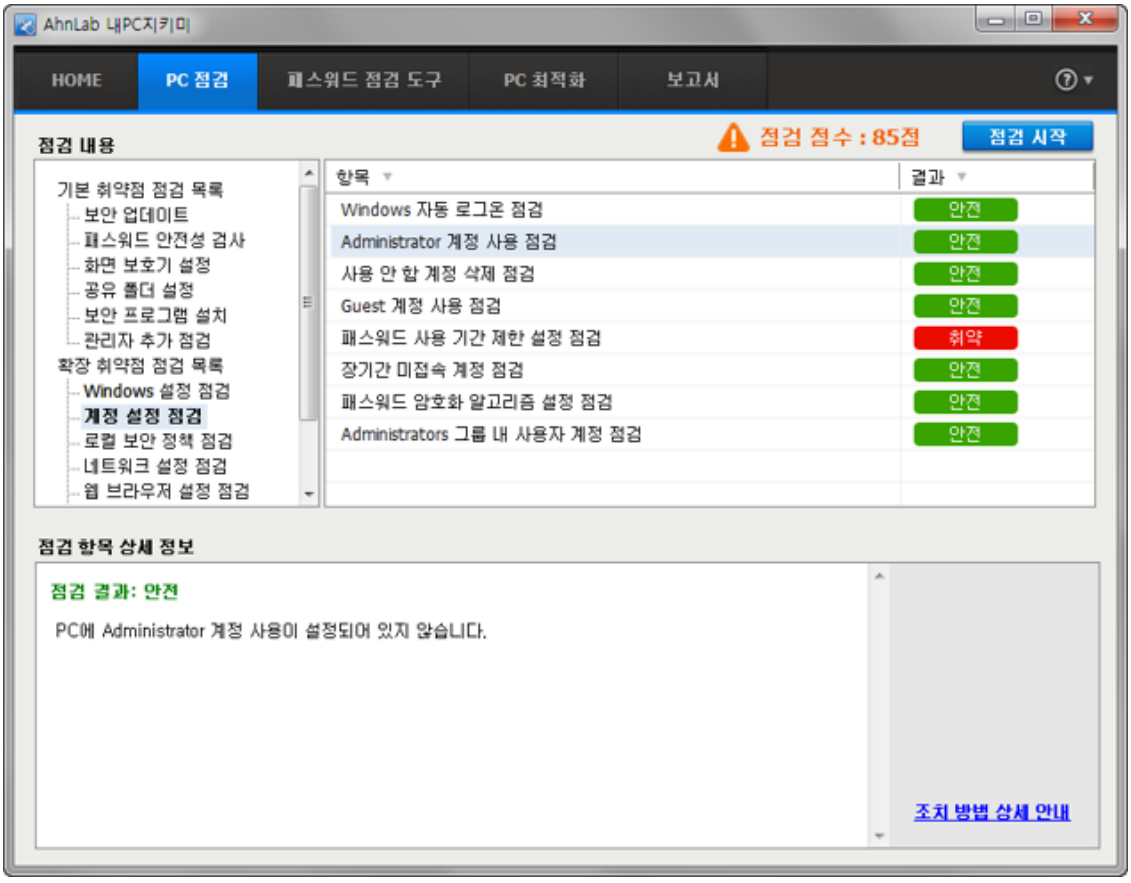
Administrator 계정 사용 점검

사용자 PC 에서 Administrator 계정을 사용하고 있는지 점검합니다.

점검 방법

Administrator 계정 사용 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 계정 설정 점검에서 **Administrator 계정 사용 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: PC 에 Administrator 이름의 계정이 존재하지 않습니다.
   - 취약: PC 에 Administrator 이름의 계정이 존재합니다. **원클릭 조치**를 눌러 Administrator 계정 이름을 변경하십시오.

조치 방법

- Administrator 계정 사용 점검

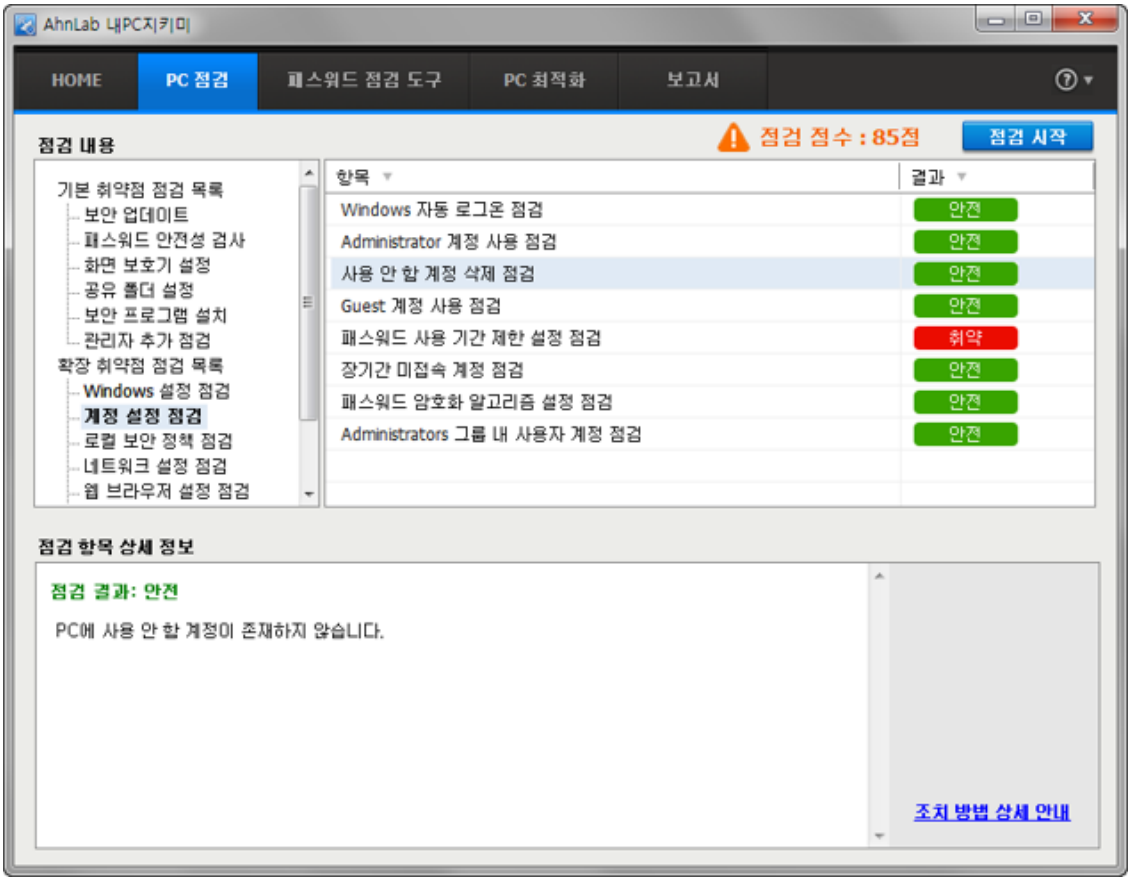
사용 안 함 계정 점검

사용자 PC 에 **사용 안 함**으로 설정된 계정이 있는지 점검합니다.

점검 방법

사용 안 함 계정의 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 계정 설정 점검에서 **사용 안 함 계정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: PC 에 **사용 안 함**으로 설정된 계정이 없습니다.
   - 취약: PC 에 **사용 안 함**으로 설정된 계정이 있는 경우입니다. 취약으로 진단된 경우, **원클릭 조치**를 눌러 사용 안 함 계정을 삭제하십시오.

조치 방법

- 사용 안 함 계정 점검

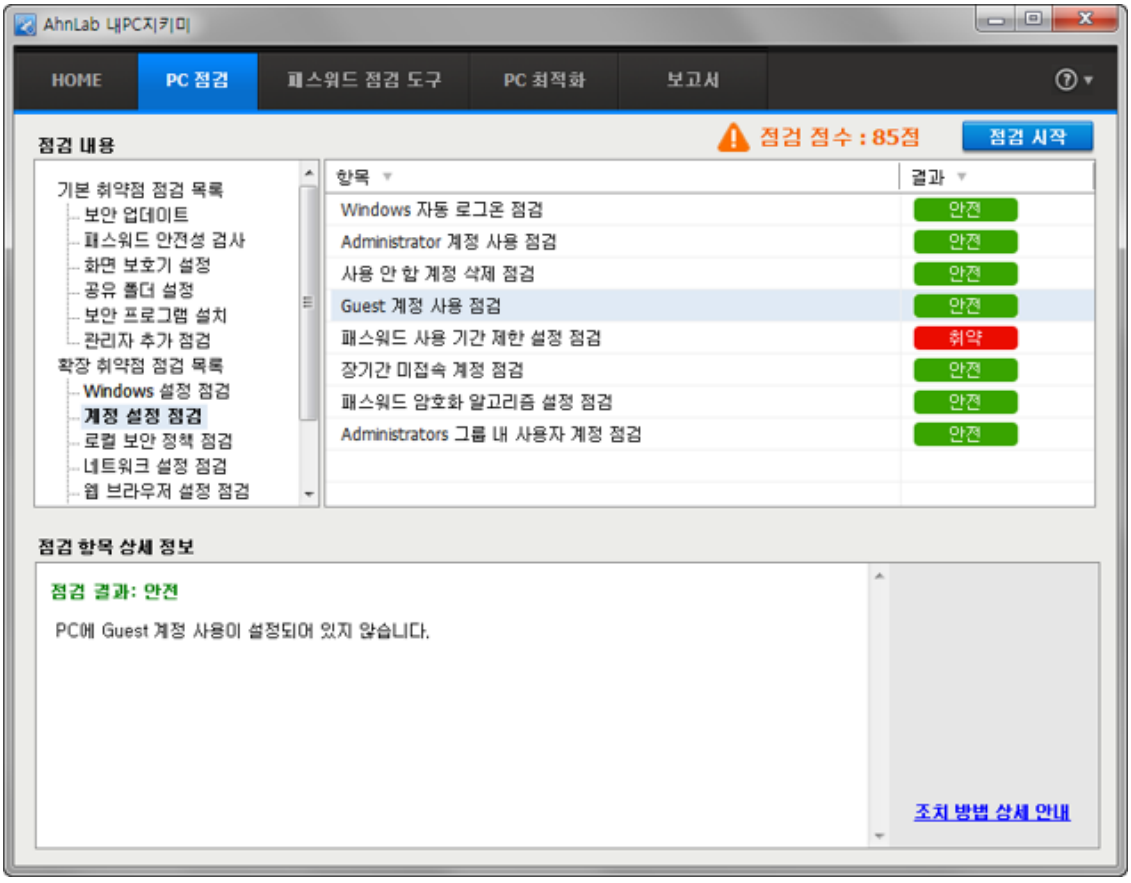
Guest 계정 사용 점검

사용자 PC 에서 Guest 계정을 사용하는 지 점검합니다.

점검 방법

Guest 계정 사용 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 계정 설정 점검에서 **Guest 계정 사용 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: Guest 이름의 계정이 존재하지 않거나 Guest 계정이 **사용 안 함**으로 설정되어 있습니다
   - 취약: Guest 이름의 계정이 사용 중입니다. Guest 계정을 **사용 안 함**으로 설정하거나 **원클릭 조치**를 눌러 Guest 계정 이름을 변경하십시오.

조치 방법

- Guest 계정 사용 점검

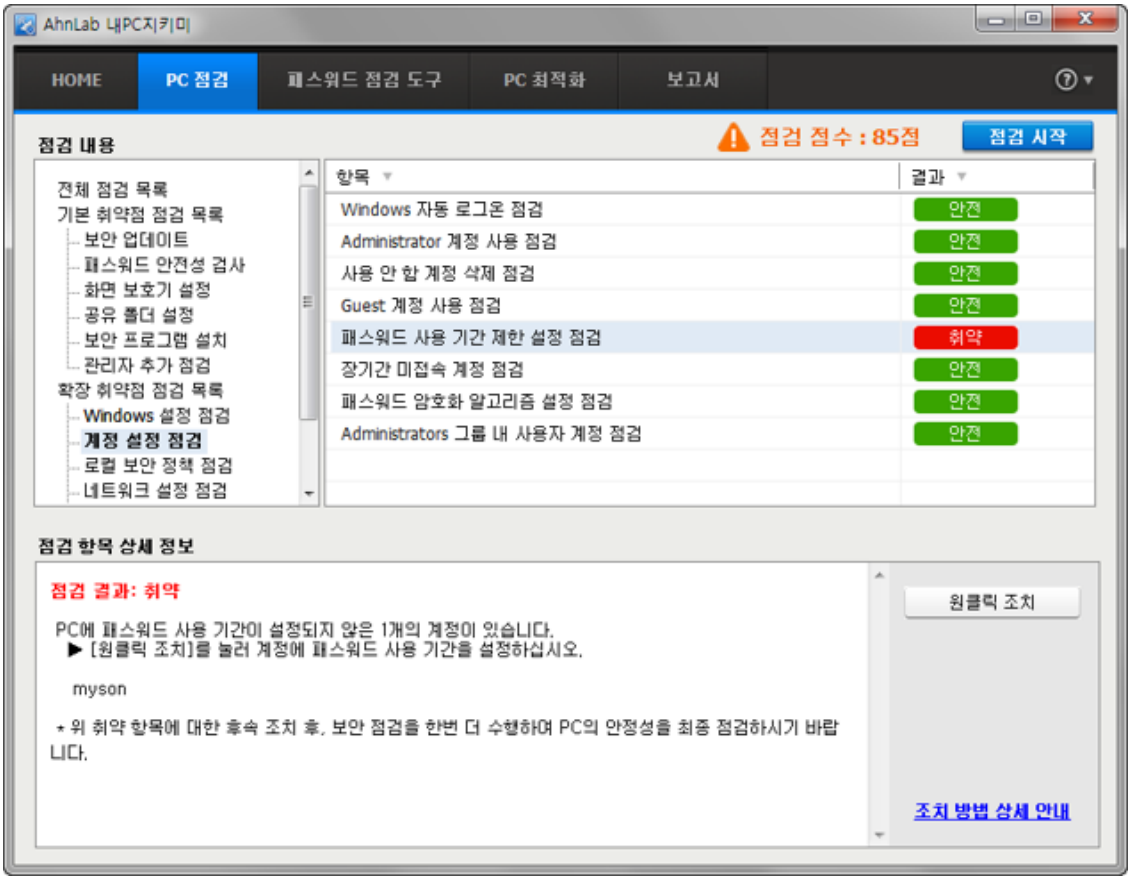
패스워드 사용 기간 제한 설정 점검

사용자 계정 패스워드에 사용 기간 제한이 설정되어 있는지 점검합니다.

점검 방법

패스워드 사용 기간 제한 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 계정 설정 점검에서 **패스워드 사용 기간 제한 설정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 사용자 계정 패스워드에 사용 기간 제한이 설정되어 있는 경우입니다.
   - 취약: 사용자 계정 패스워드에 사용 기간 제한이 설정되어 있지 않은 경우입니다. 취약으로 진단된 경우, 패스워드 사용 기간 제한이 설정되지 않은 모든 계정의 이름을 보여줍니다. **원클릭 조치**를 눌러 계정에 패스워드 사용 기간을 설정하십시오.

조치 방법

- 패스워드 사용 기간 제한 설정 점검

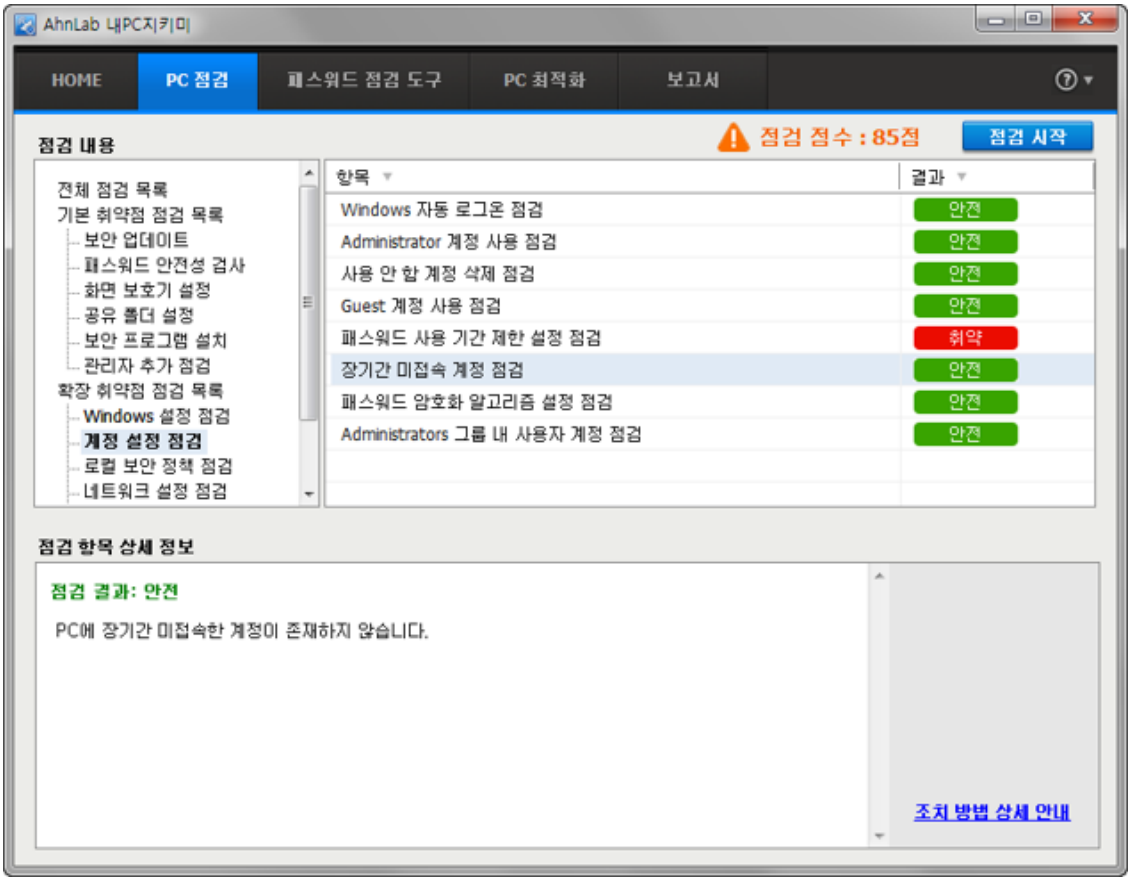
장기간 미접속 계정 점검

사용자 PC 에 장기간 접속하지 않은 사용자 계정이 존재하는지 점검합니다.

점검 방법

장기간 미접속하고 있는 계정이 존재하는 지에 대한 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 계정 설정 점검에서 **장기간 미접속 계정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 장기간 동안 접속하지 않은 계정이 존재하지 않는 경우입니다.
   - 취약: 장기간 동안 접속하지 않은 계정이 존재하는 경우입니다. 취약으로 진단된 경우, **원클릭 조치**를 눌러 관리자가 설정한 안전 조건을 초과하여 장기간 접속하지 않은 계정을 모두 삭제하십시오.

조치 방법

- 장기간 미접속 계정 점검

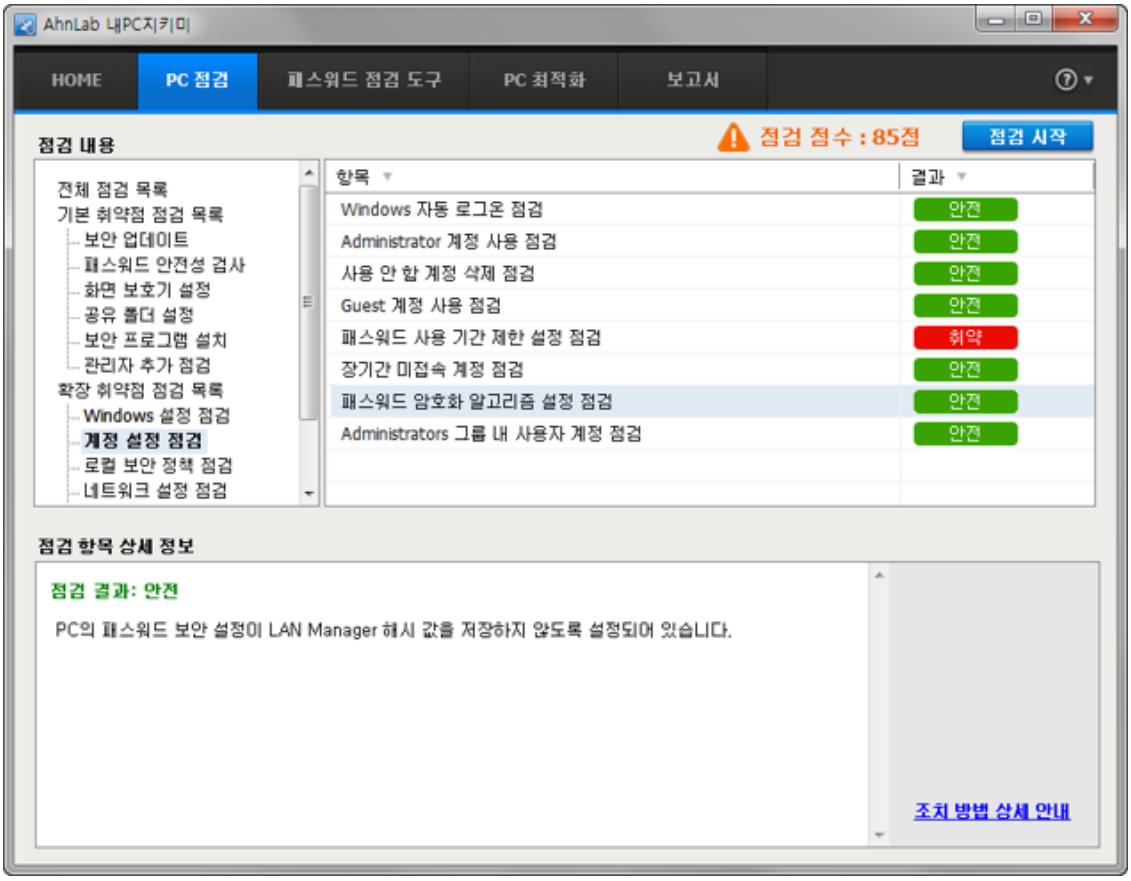
패스워드 암호화 알고리즘 설정 점검

사용자 PC 에 패스워드 암호화 알고리즘 설정이 복구 가능한 LAN Manager 해시 값을 저장하도록 설정되어 있는지 점검합니다.

점검 방법

패스워드 암호화 알고리즘 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 계정 설정 점검에서 **패스워드 암호화 알고리즘 설정 점검**을 선택합니다.



4. **패스워드 암호화 알고리즘 설정 점검** 항목을 선택하면 화면 아래에 점검 항목 상세 정보에 점검 결과가 표시됩니다.
   - 안전: 패스워드 암호화 알고리즘 설정이 LAN Manager 해시 값을 PC 에 저장하지 않도록 설정한 경우입니다.
   - 취약: 패스워드 암호화 알고리즘 설정이 LAN Manager 해시 값을 PC 에 저장하도록 설정한 경우입니다. **원클릭 조치**를 눌러 LAN Manager 해시 값을 저장하지 않도록 보안 설정을 변경하십시오.

조치 방법

- 패스워드 암호화 알고리즘 설정 점검

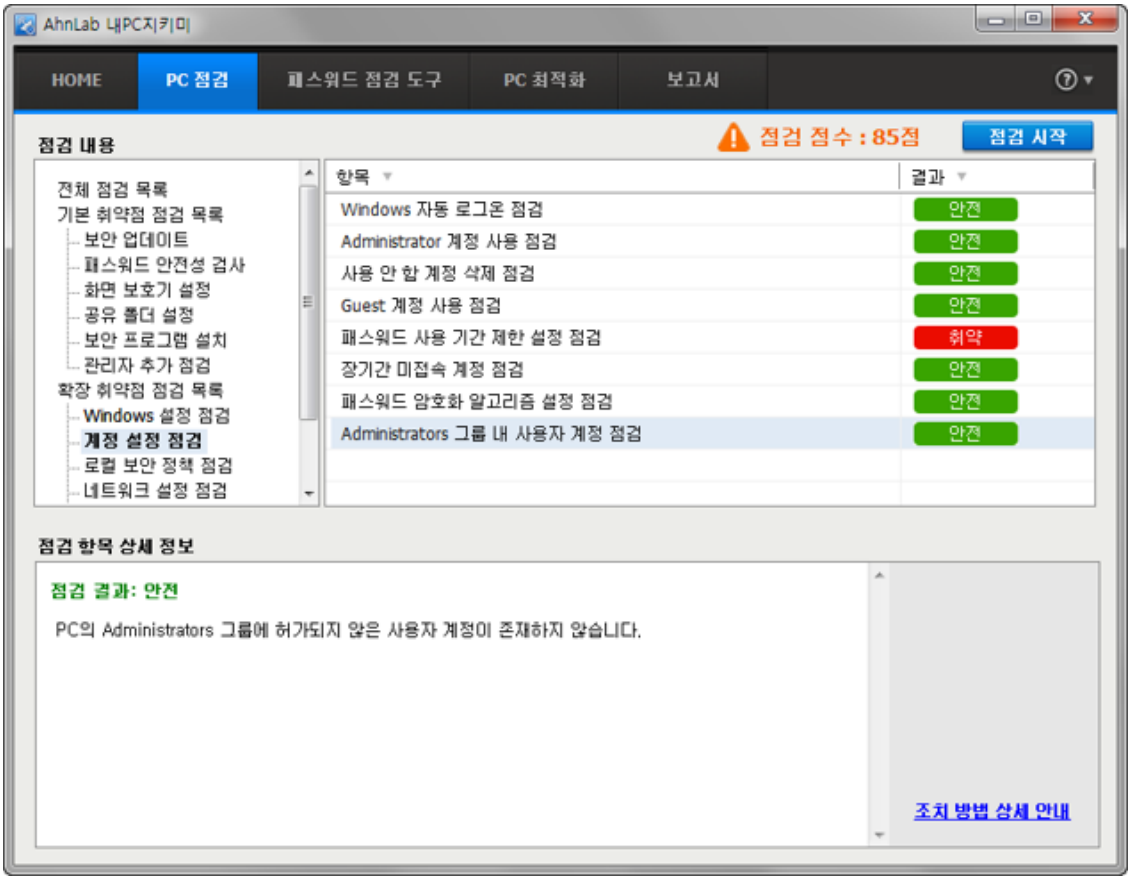
Administrators 그룹 내 사용자 계정 점검

사용자 PC 의 Administrators 그룹에 허가된 사용자만 포함되어 있는 지 점검합니다.

점검 방법

Administrators 그룹의 사용자 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 계정 설정 점검에서 **Administrators 그룹 내 사용자 계정 점검**을 선택합니다.



4. **Administrators 그룹 내 사용자 계정 점검** 항목을 선택하면 화면 아래에 점검 항목 상세 정보에 점검 결과가 표시됩니다.
   - 안전: Administrators 그룹 내에 허가된 계정 정보의 사용자만 포함되어 있습니다.
   - 취약: Administrators 그룹 내에 허가되지 않는 계정 정보가 포함되어 있는 경우입니다. **원클릭 조치**를 눌러 Administrators 그룹에 허가되지 않은 사용자 계정을 삭제하십시오.

조치 방법

- Administrators 그룹 내 사용자 계정 점검

로컬 보안 정책

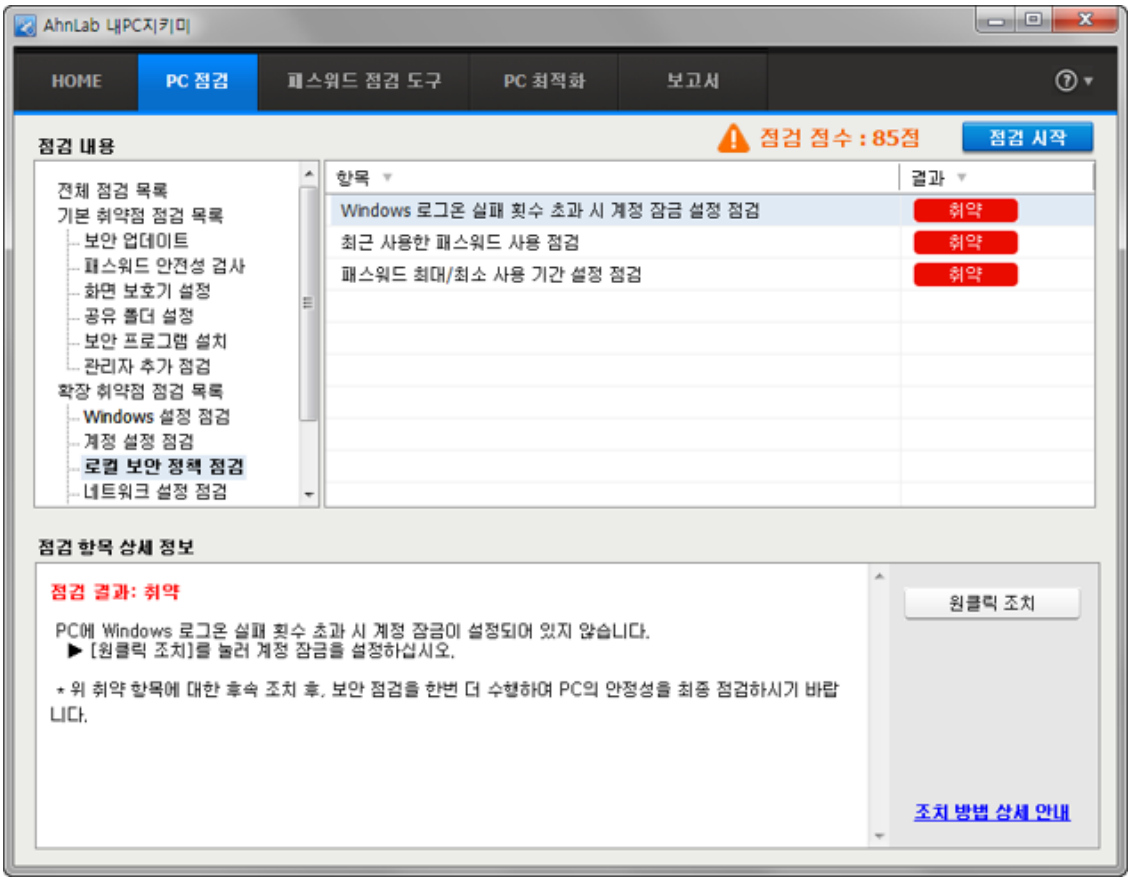
Windows 로그온 실패 횟수 초과 시 계정 잠금 설정 점검

사용자 PC 에 로그온 실패 횟수가 설정한 횟수를 초과하였을 때, 사용자 계정을 잠그도록 설정되어 있는지 점검합니다.

점검 방법

Windows 로그온 실패 횟수 초과 시 계정 잠금 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 로컬 보안 정책에서 **Windows 로그온 실패 횟수 초과 시 계정 잠금 설정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: Windows 로그온 실패 횟수 초과 시 계정 잠금이 설정된 경우입니다.
   - 취약: Windows 로그온 실패 횟수 초과 시 계정 잠금이 설정되지 않은 경우입니다. **취약**으로 진단된 경우 **원클릭 조치**를 눌러 Windows 로그온 실패 횟수 초과 시 계정 잠금이 되도록 설정해야 합니다.

조치 방법

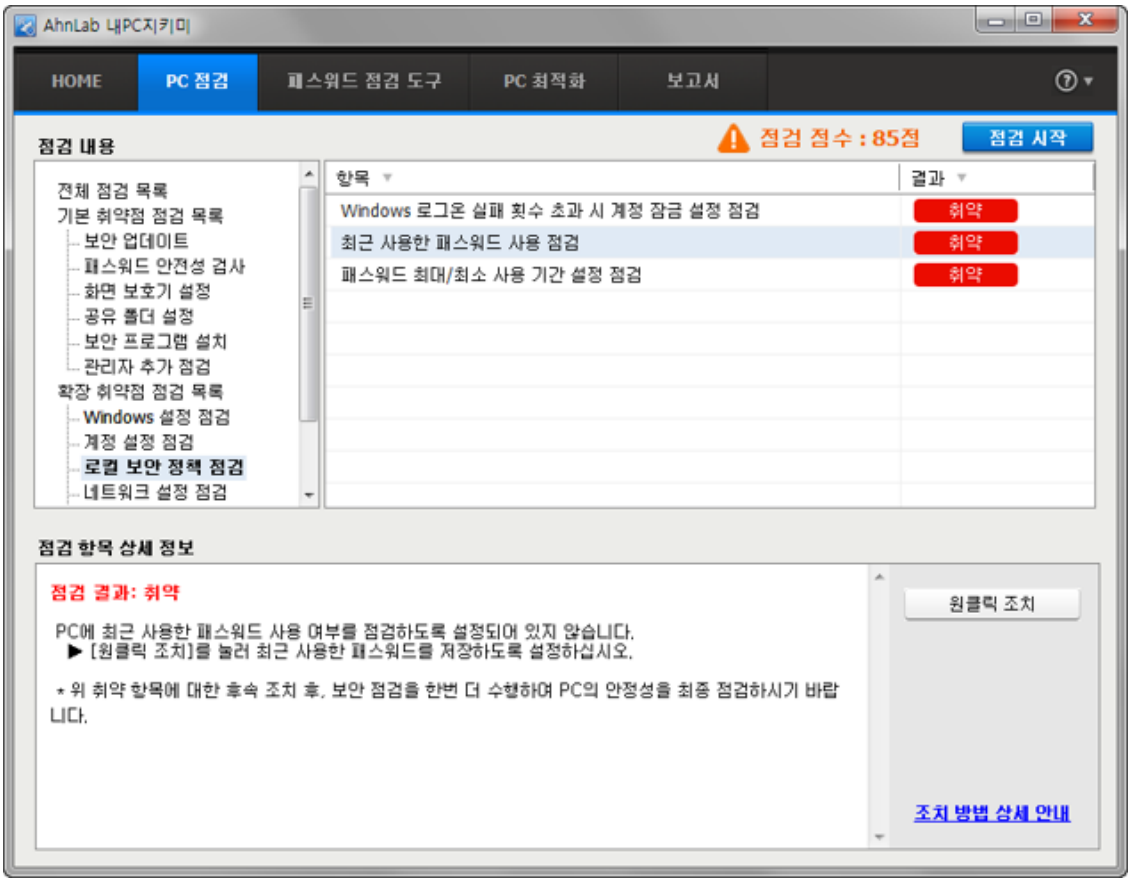
- Windows 로그온 실패 횟수 초과 시 계정 잠금 설정 점검

최근 사용한 패스워드 사용 점검

사용자가 최근 사용한 패스워드를 사용하고 있는지 알 수 있도록 최근 사용한 패스워드를 저장하고 있는지 점검합니다.

점검 방법

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 로컬 보안 정책에서 **최근 사용한 패스워드 사용 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 최근 사용한 패스워드를 저장하여 최근 사용한 패스워드를 사용하고 있는지 점검하고 있는 경우입니다.
   - 취약: 최근 사용한 패스워드를 사용하고 있는지 점검하고 있지 않은 경우입니다. 취약으로 진단된 경우, **원클릭 조치**를 눌러 최근 사용한 패스워드를 저장하도록 설정해야 합니다.

조치 방법

- 최근 사용한 패스워드 사용 점검

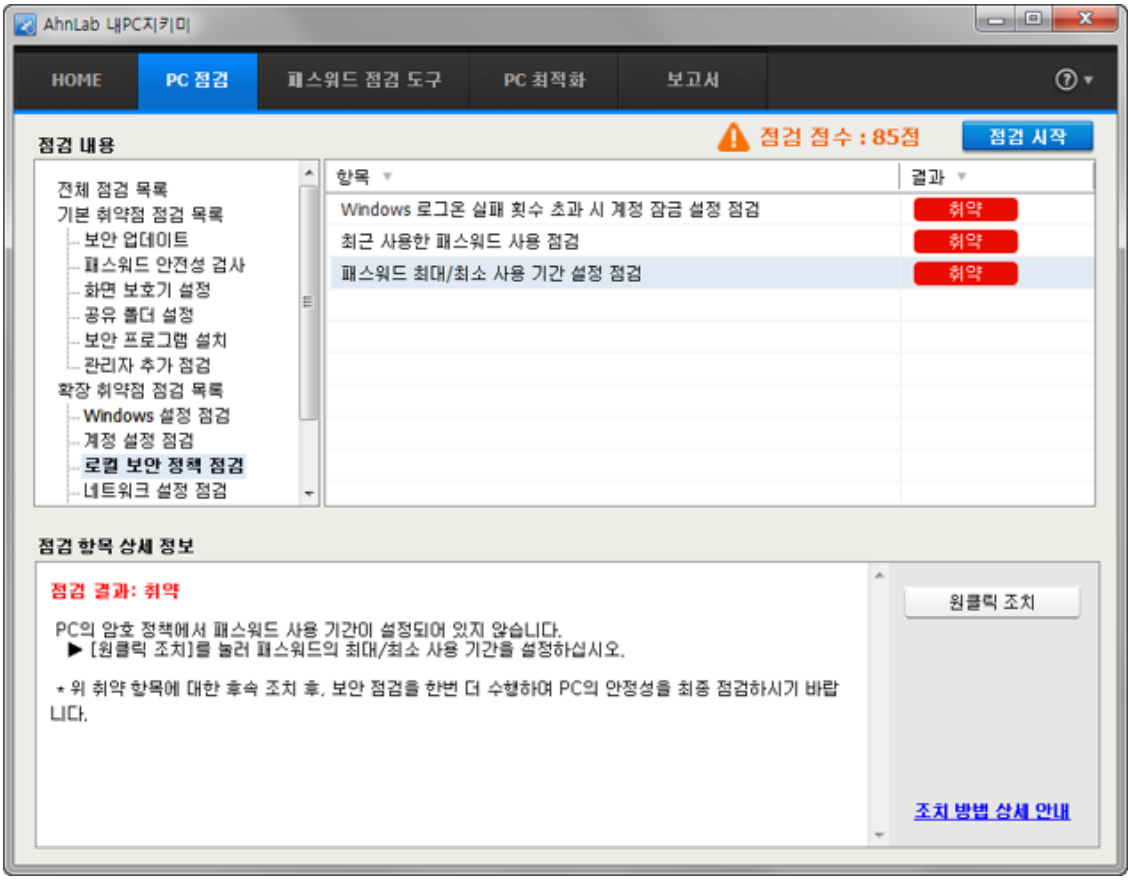
패스워드 최대/최소 사용 기간 설정 점검

사용자 계정 패스워드에 최대/최소 사용 기간이 설정되어 있는지 점검합니다.

점검 방법

패스워드 최대/최소 사용 기간 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 로컬 보안 정책에서 **패스워드 최대/최소 사용 기간 설정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 사용자 계정 패스워드에 최대/최소 사용 기간이 설정되어 있는 경우입니다.
   - 취약: 사용자 계정 패스워드에 최대/최소 사용 기간이 설정되어 있지 않은 경우입니다. 취약으로 진단된 경우 **원클릭 조치**를 눌러 관리자가 설정한 패스워드의 최대/최소 사용 기간을 사용자 PC 에 설정해야 합니다.

조치 방법

- 패스워드 최대/최소 사용 기간 설정 점검

네트워크 설정 점검

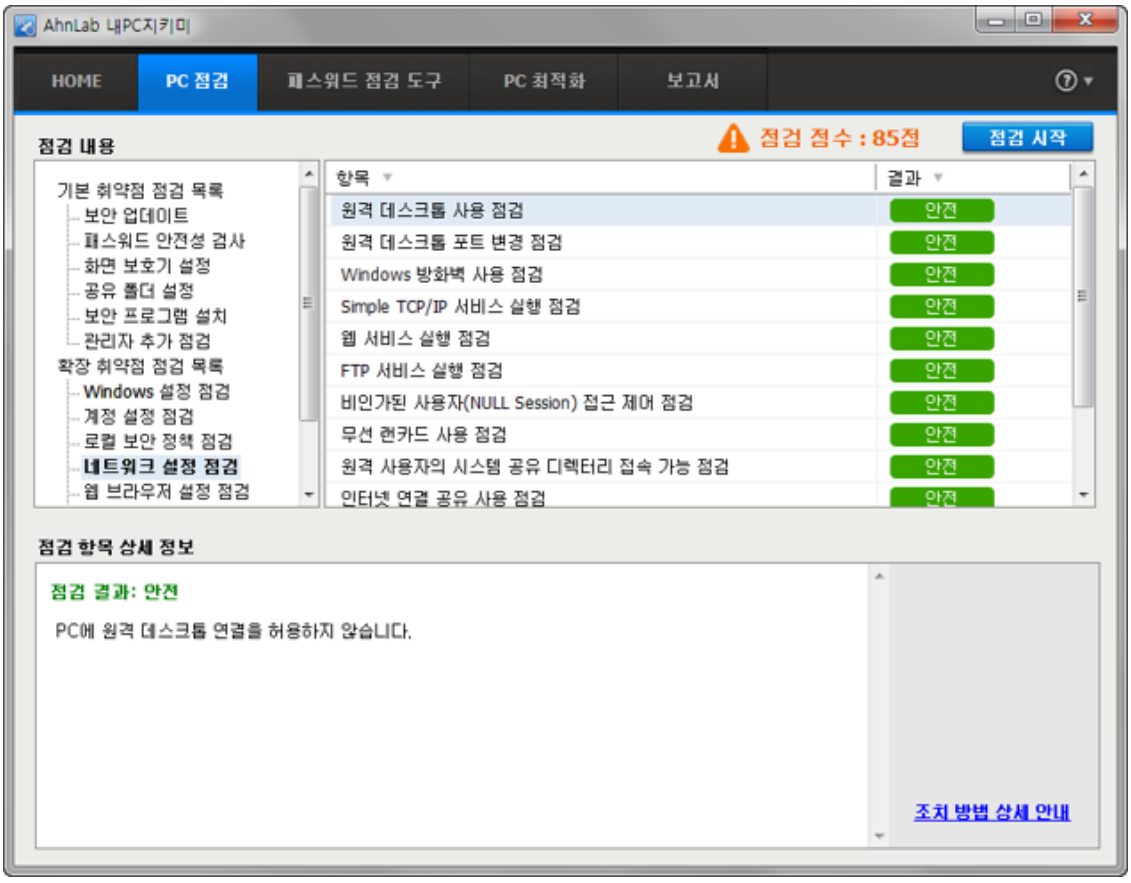
원격 데스크톱 사용 점검

사용자 PC 에 원격 데스크톱 연결을 허용하도록 설정되어 있는지 점검합니다.

점검 방법

원격 데스크톱 사용 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 **원격 데스크톱 사용 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 원격 데스크톱 연결이 설정되어 있지 않은 경우입니다.
   - 취약: 원격 데스크톱 연결이 설정되어 있는 경우입니다. 취약으로 진단된 경우, **원클릭 조치**를 눌러 원격 데스크톱 연결 설정을 해제하십시오.

조치 방법

- 원격 데스크톱 사용 점검

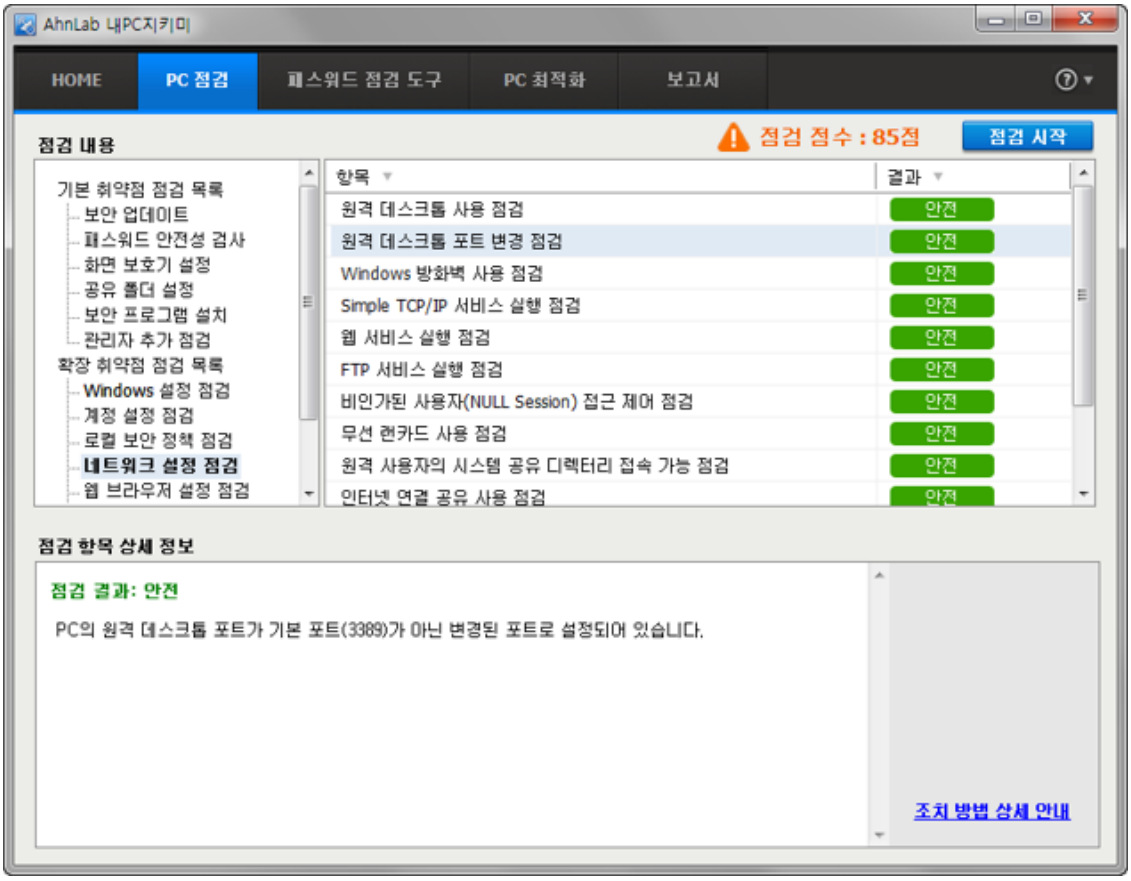
원격 데스크톱 포트 변경 점검

사용자 PC 에 원격 데스크톱 포트가 변경되지 않고, 기본 포트(3389)로 유지되고 있는지 점검합니다.

점검 방법

원격 데스크톱 포트 변경 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 **원격 데스크톱 포트 변경 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 원격 데스크톱 포트가 기본 포트 번호에서 변경되어 있습니다.
   - 취약: 원격 데스크톱 포트가 기본 포트인 3389 번으로 설정되어 있습니다. **원클릭 조치**를 눌러 원격 데스크톱 포트를 변경하십시오.

조치 방법

- 원격 데스크톱 포트 변경 점검

Windows 방화벽 사용 점검

사용자 PC 에 Windows 방화벽을 사용하도록 설정되어 있는지 점검합니다.

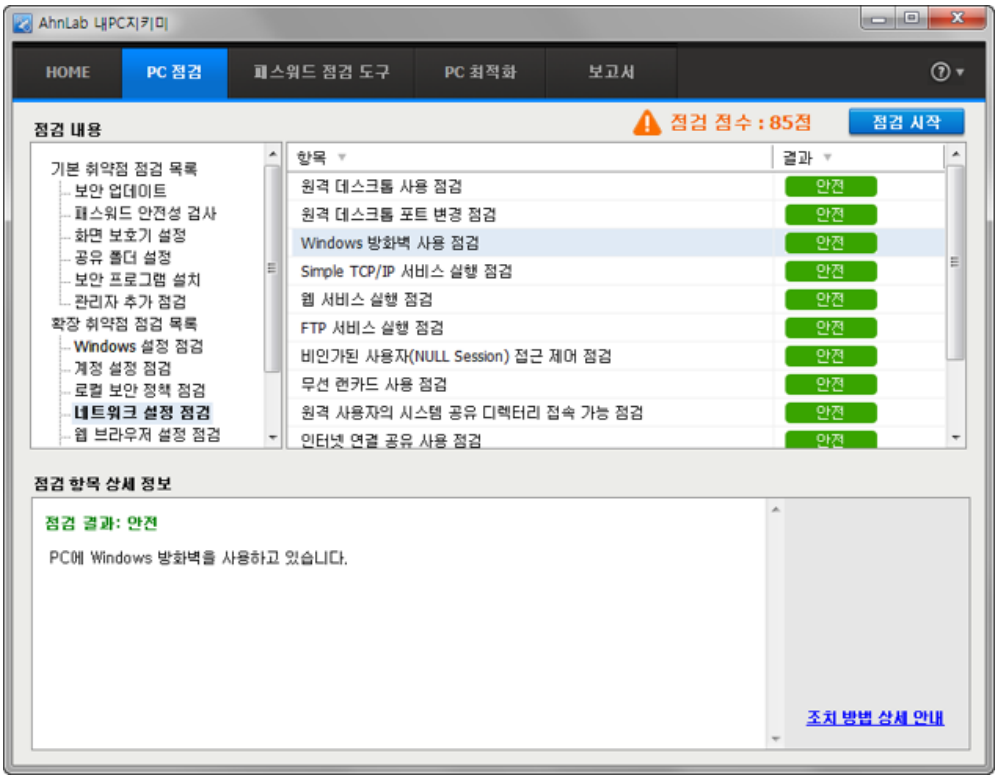
Windows 방화벽

방화벽은 인터넷 또는 네트워크에서 들어오는 정보를 확인한 다음 방화벽 설정에 따라 이를 컴퓨터로 전달하는 것을 차단하거나 허용하는 소프트웨어 또는 하드웨어입니다. 방화벽은 해커 또는 악성 소프트웨어(예: 웜)가 네트워크나 인터넷을 통해 사용자 컴퓨터에 액세스하지 못하도록 방지합니다. 또한 사용자 컴퓨터에서 다른 컴퓨터로 악성 소프트웨어를 보내지 못하도록 방지할 수 있습니다. 방화벽은 바이러스 백신 프로그램과 동일하지 않습니다. 컴퓨터를 안전하게 보호하려면 방화벽, 바이러스 백신 및 맬웨어 방지 프로그램이 모두 필요합니다. Windows 방화벽 사용 여부를 점검하는 방법은 다음과 같습니다.

점검 방법

Windows 방화벽 사용 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 **Windows 방화벽 사용 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: Windows 방화벽을 사용하도록 설정되어 있습니다.
   - 취약: Windows 방화벽을 사용하고 있지 않습니다. **원클릭 조치**를 눌러 Windows 방화벽을 사용하도록 조치하십시오.

조치 방법

- Windows 방화벽 사용 점검

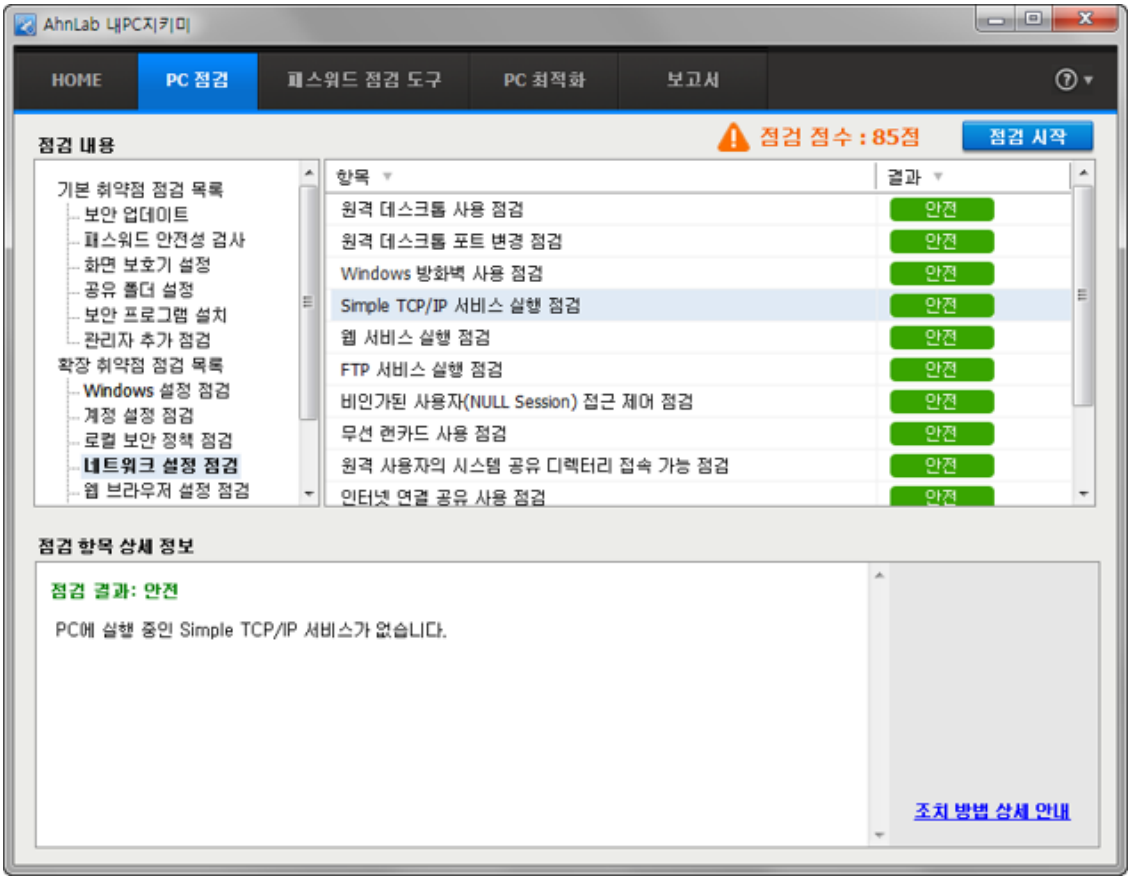
Simple TCP/IP 서비스 실행 점검

사용자 PC 에 Simple TCP/IP 서비스가 실행되고 있는지 점검합니다.

점검 방법

Simple TCP/IP 서비스의 실행 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 **Simple TCP/IP 서비스 실행 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: PC 에 Simple TCP/IP 서비스가 실행 중이지 않은 경우입니다.
   - 취약: PC 에 Simple TCP/IP 서비스가 실행 중입니다. **원클릭 조치**를 눌러 Simple TCP/IP 서비스를 중지하십시오.

조치 방법

- Simple TCP/IP 서비스 실행 점검

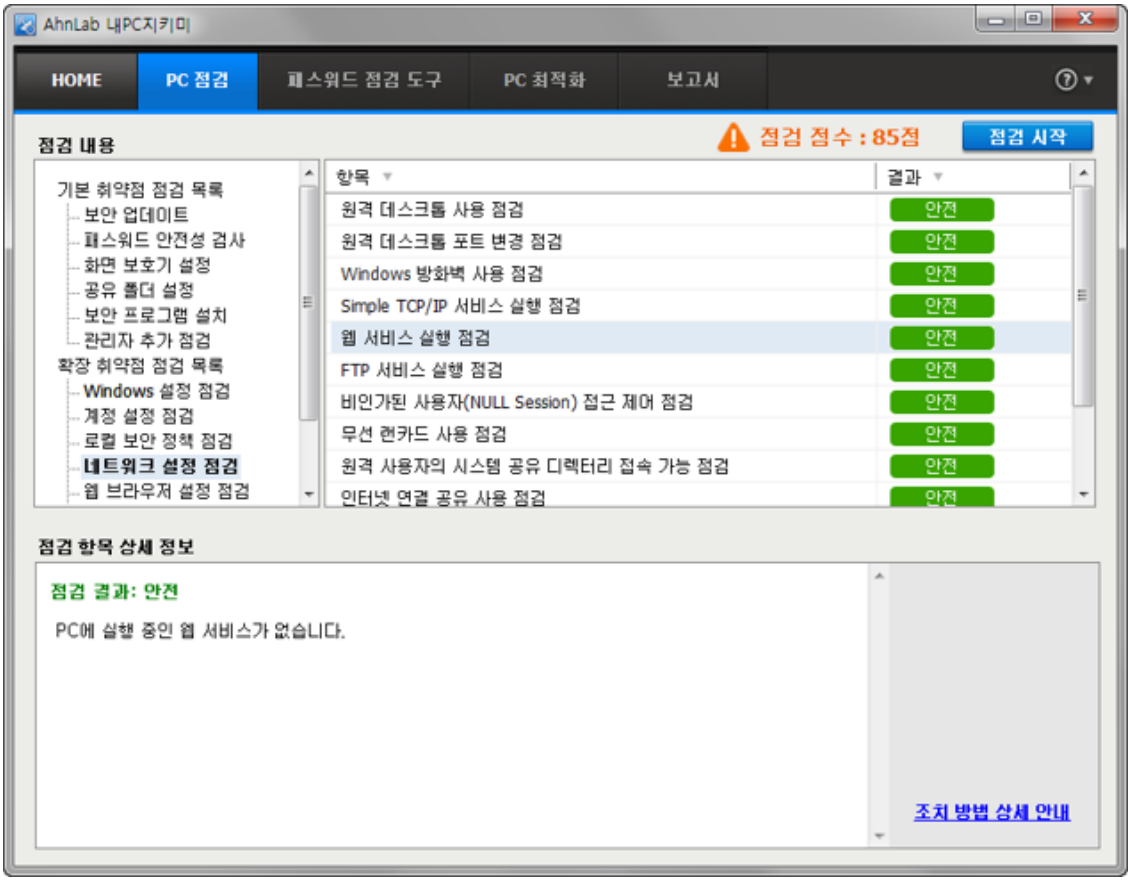
웹 서비스 실행 점검

사용자 PC 에 웹 서비스가 실행 중인지 점검합니다.

점검 방법

웹 서비스 실행 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 **웹 서비스 실행 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: PC 에 실행 중인 웹 서비스가 없습니다.
   - 취약: PC 에 웹 서비스가 실행 중입니다. **원클릭 조치**를 눌러 웹 서비스를 중지하십시오.

조치 방법

- 웹 서비스 실행 점검

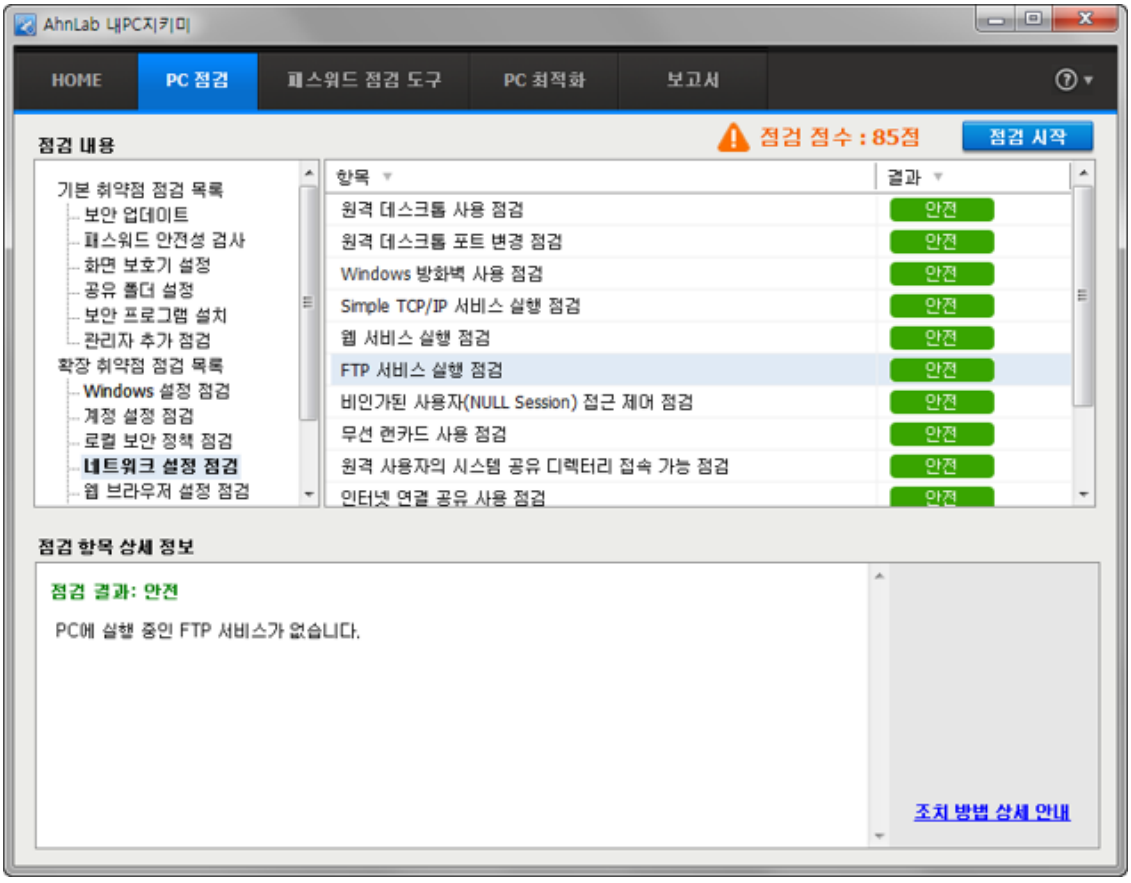
FTP 서비스 실행 점검

사용자 PC 에 FTP 서비스가 실행 중인지 점검합니다.

점검 방법

FTP 서비스 실행 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 **FTP 서비스 실행 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: PC 에 실행 중인 FTP 서비스가 없습니다.
   - 취약: PC 에 FTP 서비스가 실행 중입니다. **원클릭 조치**를 눌러 FTP 서비스를 중지하십시오.

조치 방법

- FTP 서비스 실행 점검

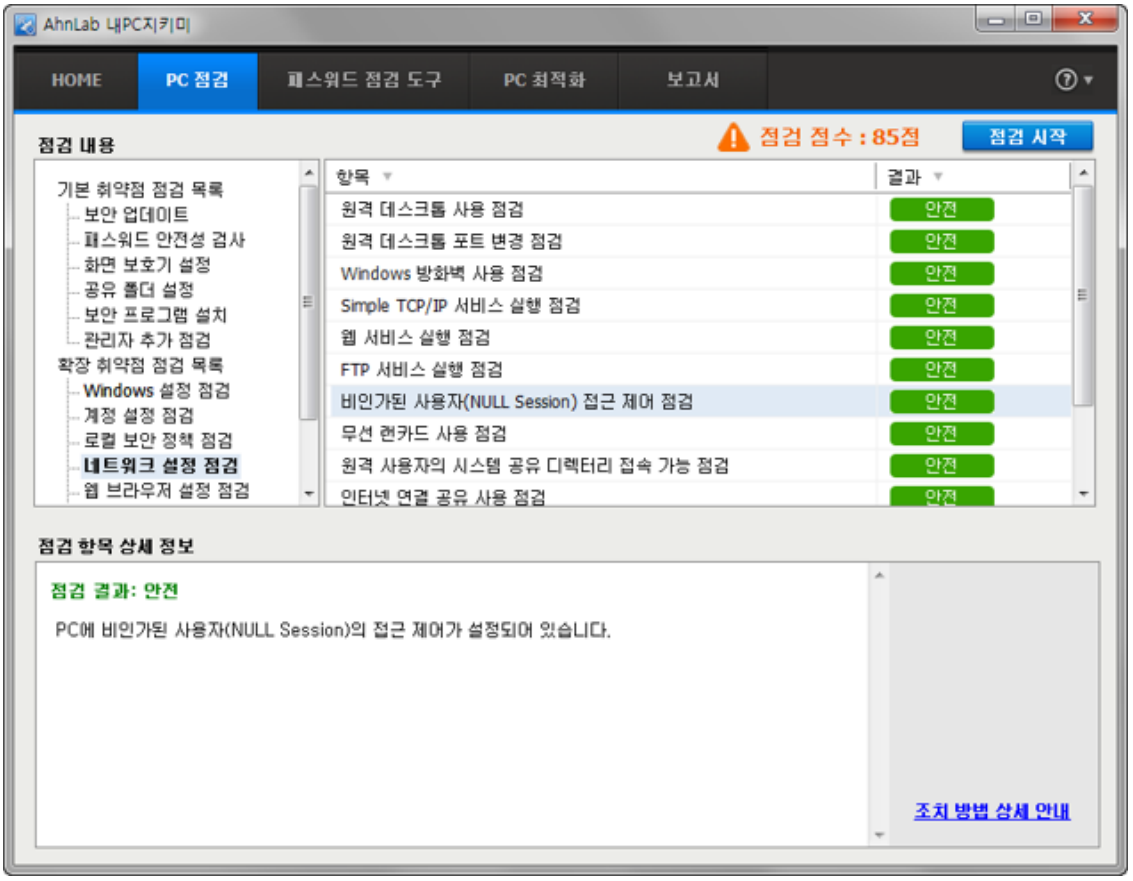
비인가된 사용자(NULL Session) 접근 제어 점검

사용자 PC 에 비인가된 사용자(NULL Session)가 접근했을 때, 접근 제어가 설정되어 있는지 점검합니다.

점검 방법

비인가 사용자 접근 제어(NULL Session 접근 제어) 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 비인가된 사용자(NULL Session) 접근 제어 점검을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: PC 에 비인가된 사용자(NULL Session)의 접근 제어가 설정되어 있습니다.
   - 취약: PC 에 비인가된 사용자(NULL Session)의 접근을 허용하도록 설정되어 있습니다. **원클릭 조치**를 눌러 비인가 사용자에 대한 접근을 허용하지 않도록 설정하십시오.

조치 방법

- 비인가 사용자 접근 제어(NULL Session 접근 제어) 점검

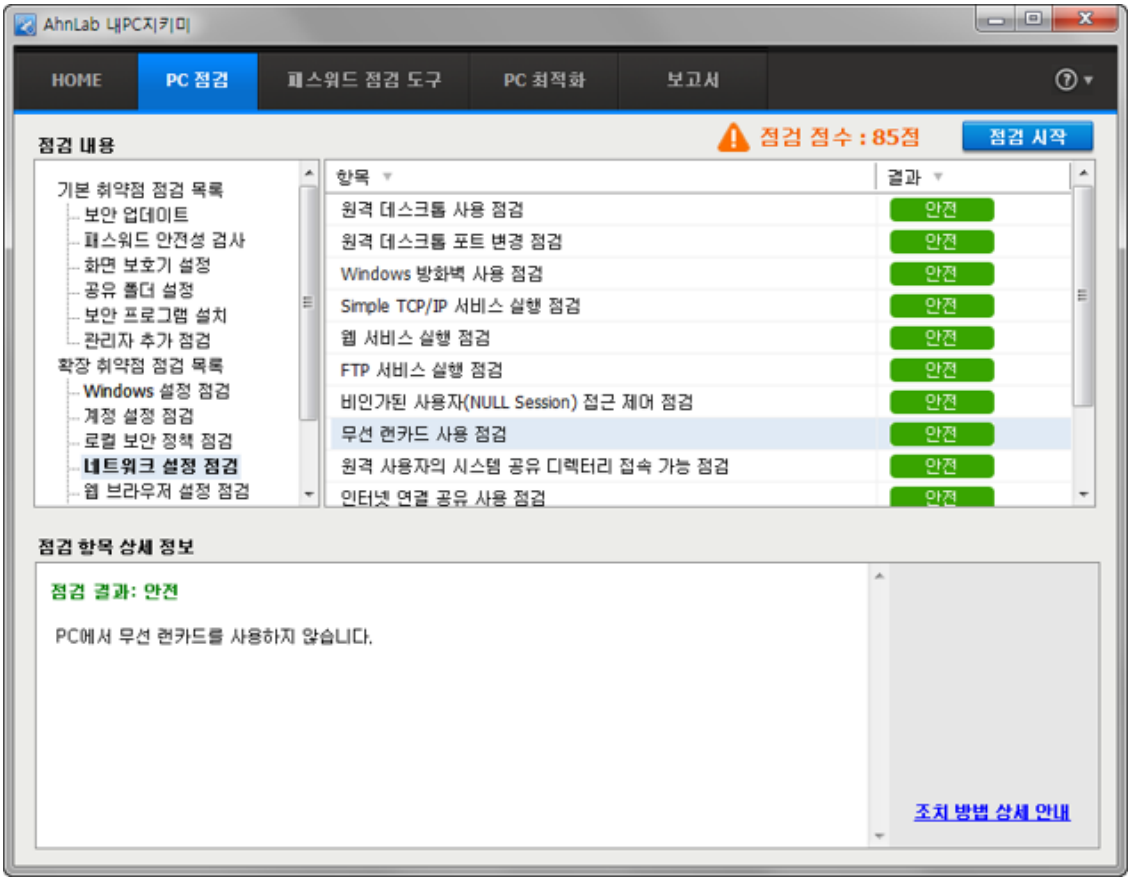
무선 랜카드 사용 점검

사용자 PC 에 무선 랜카드를 사용하고 있는지 점검합니다.

점검 방법

무선 랜카드 사용 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 **무선 랜카드 사용 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: PC 에서 무선 랜카드를 사용하지 않습니다.
   - 취약: PC 에서 무선 랜카드를 사용하고 있습니다. **원클릭 조치**를 눌러 무선 랜카드 사용을 중지하십시오.

조치 방법

- 무선 랜카드 사용 점검

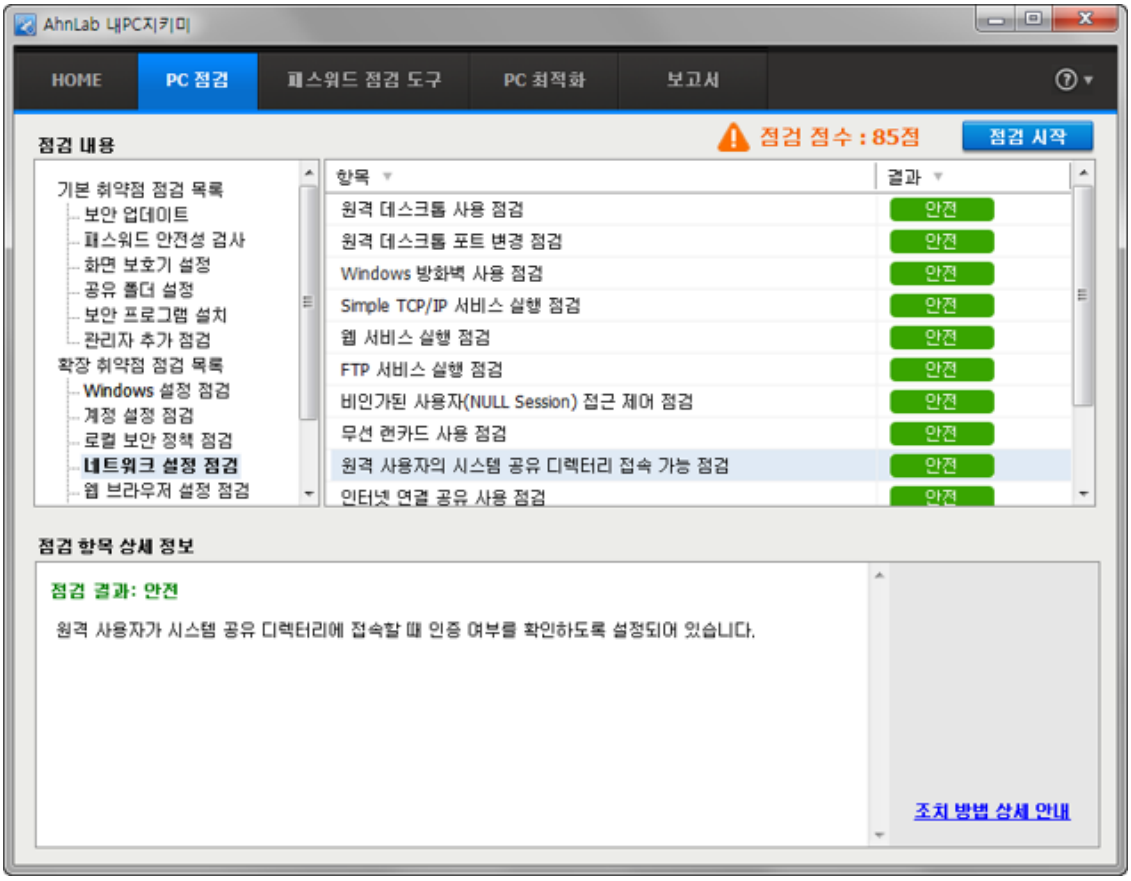
원격 사용자의 시스템 공유 디렉터리 접속 가능 점검

사용자 PC 에 원격에서 사용자 인증 없이 시스템 공유 디렉터리에 접속할 때 차단 여부를 확인하도록 설정되어 있는지 점검합니다.

점검 방법

원격 사용자의 시스템 공유 디렉터리 접속 가능 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 원격 사용자 인증의 시스템 공유 디렉터리 접속 가능 점검을 선택합니다.



4. **원격 사용자 인증의 시스템 공유 디렉터리 접속 가능 점검** 항목을 선택하면 화면 아래에 점검 항목 상세 정보에 점검 결과가 표시됩니다.
   - 안전: 원격에서 사용자가 인증 없이 시스템 공유 디렉터리에 접속하는 것을 차단하도록 네트워크 액세스 권한이 설정되어 있는 경우입니다.
   - 취약: 원격 사용자가 인증 없이 시스템 공유 디렉터리에 접속할 수 있게 설정되어 있습니다. **원클릭 조치**를 눌러 원격 사용자가 인증 없이 시스템 공유 디렉터리에 접속할 수 없도록 설정하십시오.

조치 방법

- 원격 사용자의 시스템 공유 디렉터리 접속 가능 점검

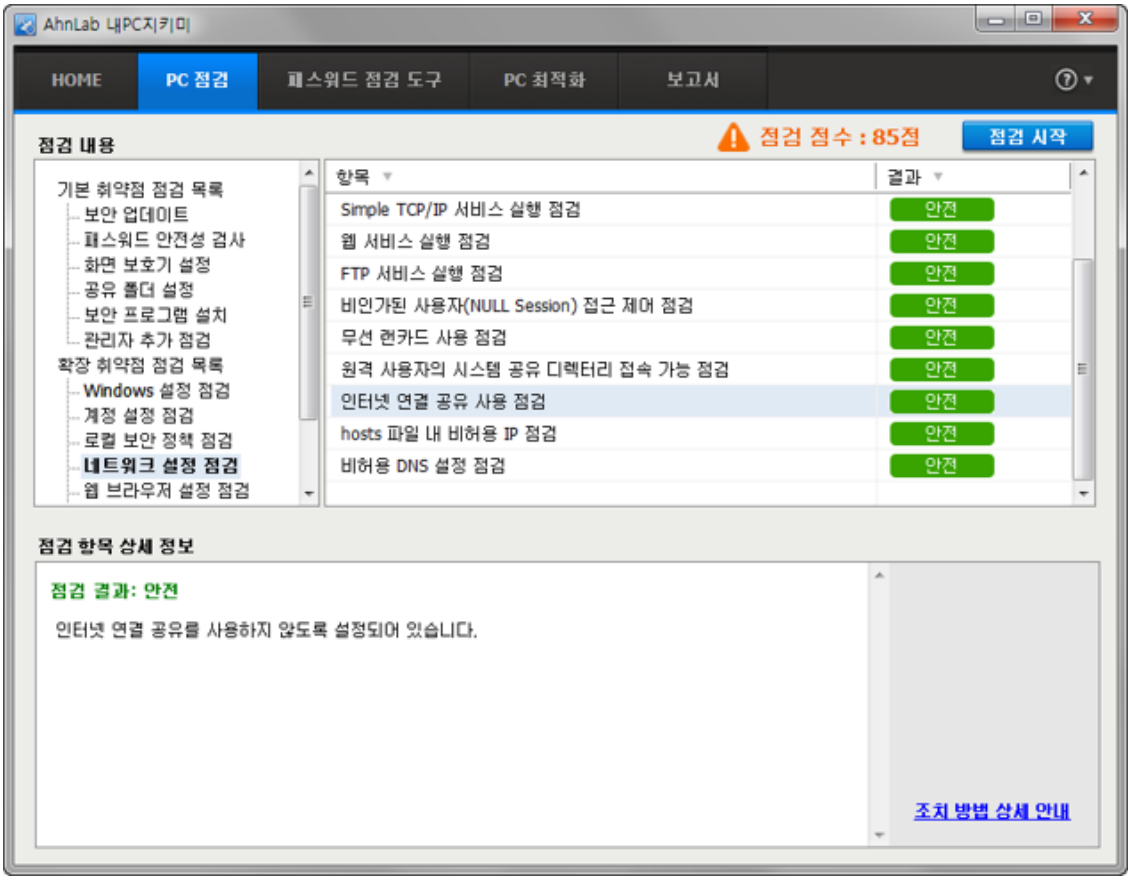
인터넷 연결 공유 사용 점검

에이전트 PC 의 인터넷 연결 공유 설정이 다른 네트워크 사용자가 에이전트 PC 의 인터넷 연결을 공유하여 사용할 수 있도록 설정되어 있는 지 점검합니다.

점검 방법

인터넷 연결 공유 사용 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 **인터넷 연결 공유 사용 점검**을 선택합니다.



4. **인터넷 연결 공유 사용 점검** 항목을 선택하면 점검 항목 상세 정보에 점검 결과가 표시됩니다.
   - 안전: 에이전트 PC 설정이 인터넷 연결 공유를 사용하지 않도록 설정되어 있습니다.
   - 취약: 에이전트 PC 설정이 인터넷 연결 공유를 사용하도록 설정되어 있습니다. **원클릭 조치**를 눌러 다른 네트워크 사용자가 에이전트 PC 의 인터넷 연결 공유 기능을 사용할 수 없도록 설정하십시오.

조치 방법

- 인터넷 연결 공유 사용 점검

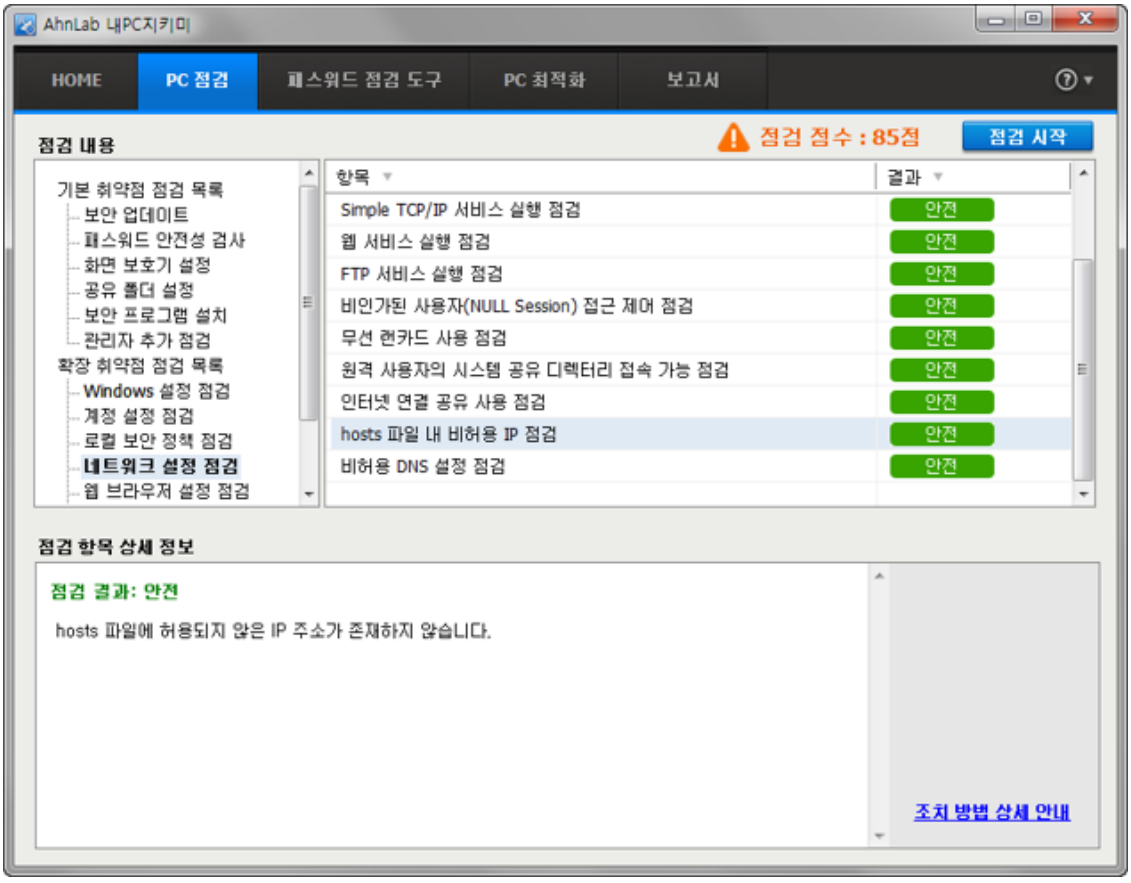
hosts 파일 내 비허용 IP 점검

hosts 파일에 허용되지 않은 IP 주소가 설정되어 있는 지 점검합니다.

점검 방법

hosts 파일 내 비허용 IP 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 **hosts 파일 내 비허용 IP 점검**을 선택합니다.



4. **hosts 파일 내 비허용 IP 점검** 항목을 선택하면 점검 항목 상세 정보에 점검 결과가 표시됩니다.
   - 안전: hosts 파일에 허용되지 않은 IP 주소가 존재하지 않습니다.
   - 취약: hosts 파일에 허용되지 않은 IP 주소가 %d 개 있습니다. **원클릭 조치**를 눌러 허용되지 않은 IP 주소를 사용하지 않도록 설정하십시오.

조치 방법

- hosts 파일 내 비허용 IP 점검

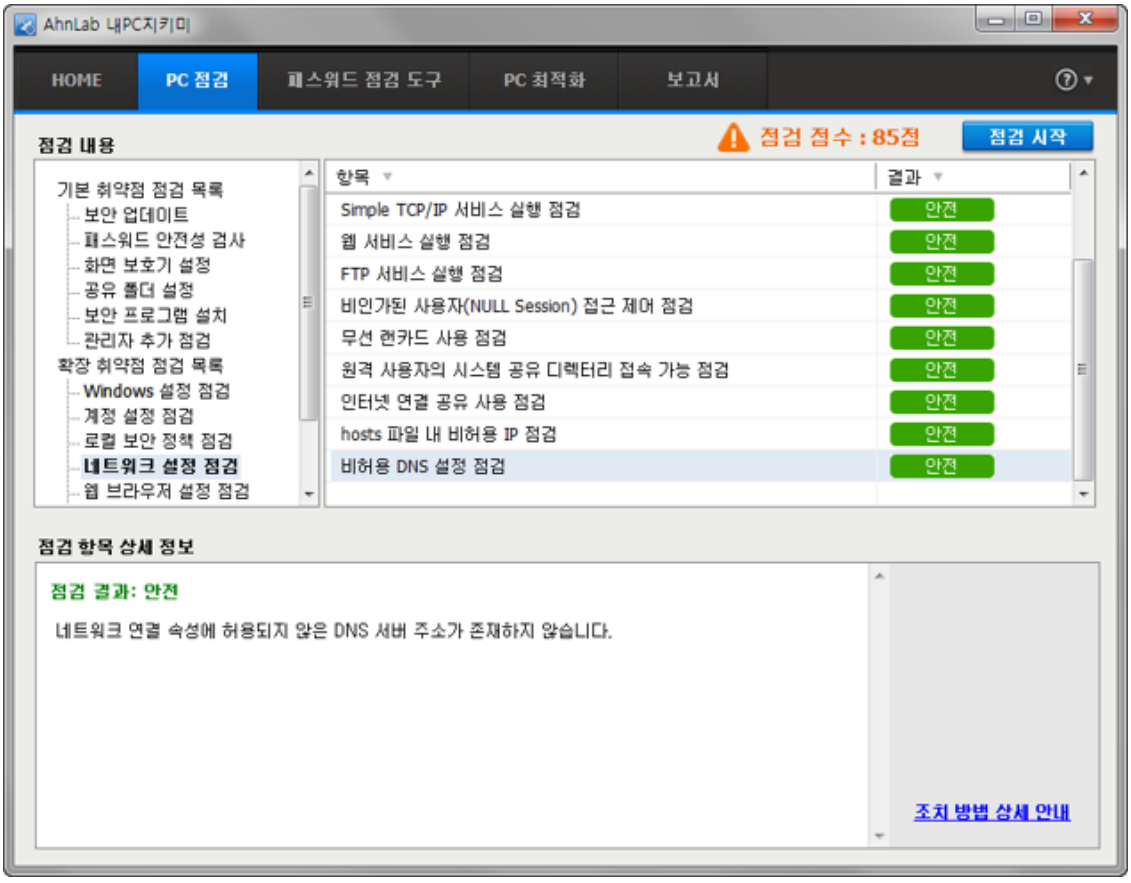
비허용 DNS 설정 점검

네트워크 연결 속성에 허용되지 않은 DNS 서버 주소가 설정되어 있는 지 점검합니다.

점검 방법

비허용 DNS 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 **비허용 DNS 설정 점검**을 선택합니다.



4. **비허용 DNS 설정 점검** 항목을 선택하면 점검 항목 상세 정보에 점검 결과가 표시됩니다.
   - 안전: 네트워크 연결 속성에 허용되지 않은 DNS 서버 주소가 존재하지 않습니다.
   - 취약: 네트워크 연결 속성에 허용되지 않은 DNS 서버 주소가 있습니다. **조치 방법 상세 안내**를 참고하여 허용되지 않은 DNS 서버 주소를 사용하지 않도록 설정하십시오.

조치 방법

- 비허용 DNS 설정 점검

웹 브라우저 설정 점검

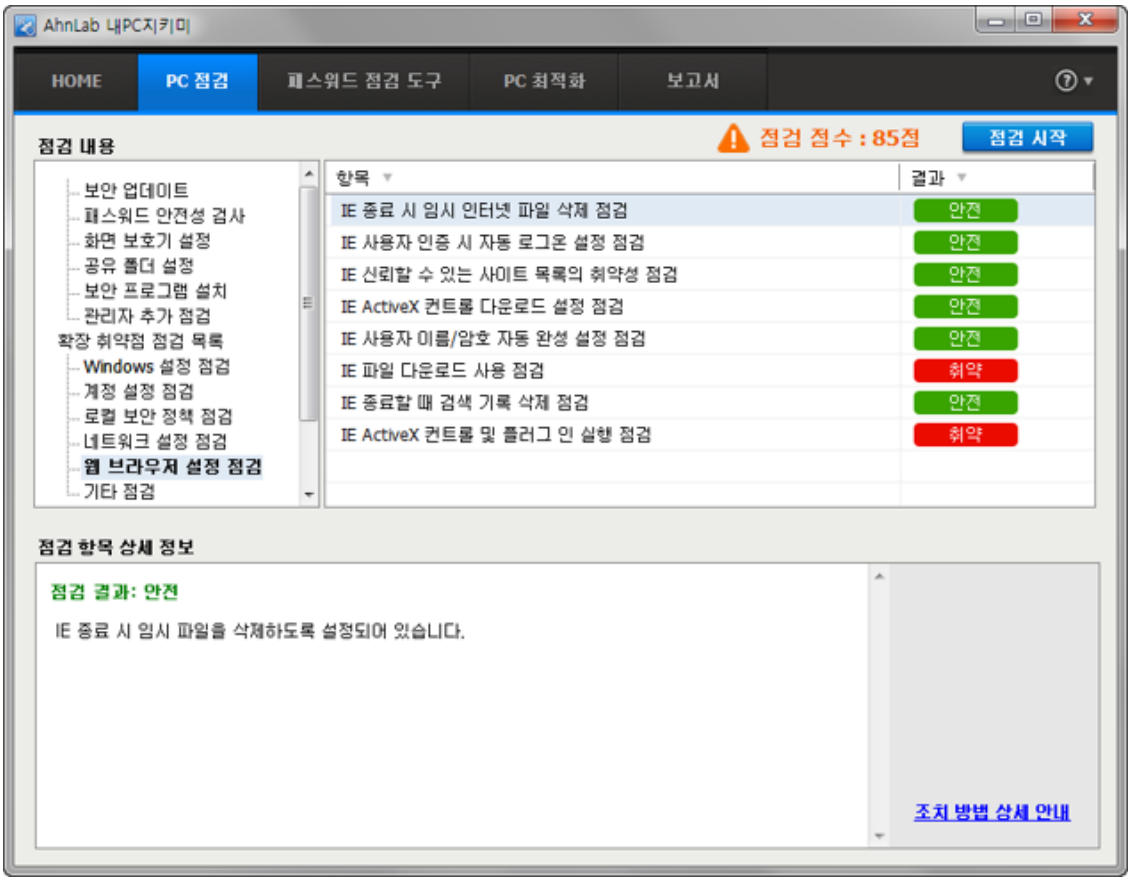
IE 종료 시 임시 인터넷 파일 삭제 점검

인터넷 옵션에서 IE 를 종료할 때 임시 인터넷 파일을 삭제하도록 설정되어 있는지 점검합니다.

점검 방법

IE 종료 시 임시 인터넷 파일 삭제 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내PC지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 **IE 종료 시 임시 인터넷 파일 삭제 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: IE 종료 시 임시 파일을 삭제하도록 설정되어 있습니다.
   - 취약: IE 종료 시 임시 파일 삭제 설정이 되어 있지 않습니다. **원클릭 조치**를 눌러 IE 종료 시 임시 파일을 삭제하도록 설정하십시오.

조치 방법

- IE 종료 시 임시 인터넷 파일 삭제 점검

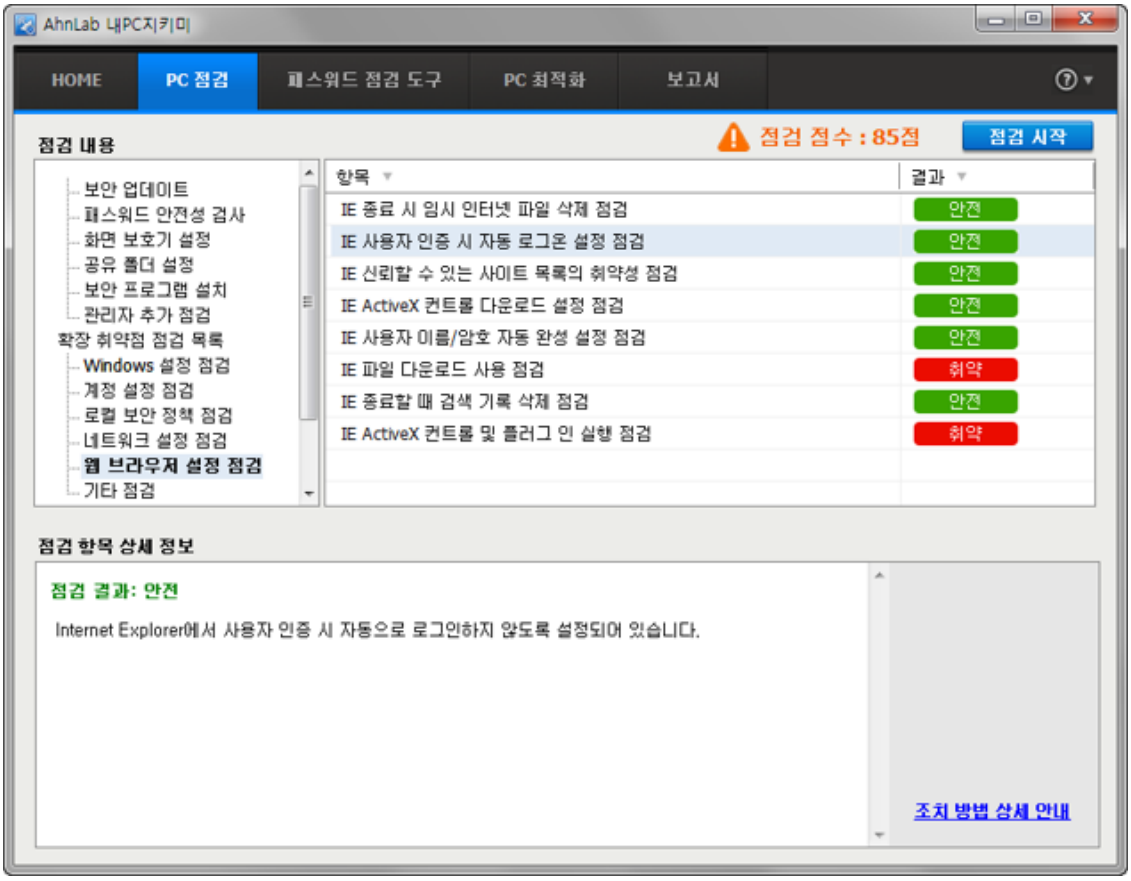
IE 사용자 인증 시 자동 로그온 설정 점검

IE 에서 사용자 인증을 요구할 때, 사용자 계정과 암호가 저장되어 자동으로 로그온할 수 있도록 설정되어 있는지 점검합니다.

점검 방법

IE 사용자 인증 시 자동 로그온 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 **IE 사용자 인증 시 자동으로 로그온 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: IE 에서 사용자 인증 시 자동으로 로그인하지 않도록 설정되어 있습니다.
   - 취약: IE 에서 사용자 인증 시 자동으로 로그인 하도록 설정되어 있습니다. **원클릭 조치**를 눌러 사용자 인증 시 자동으로 로그인하지 않도록 설정하십시오.

조치 방법

- IE 사용자 인증 시 자동 로그온 설정 점검

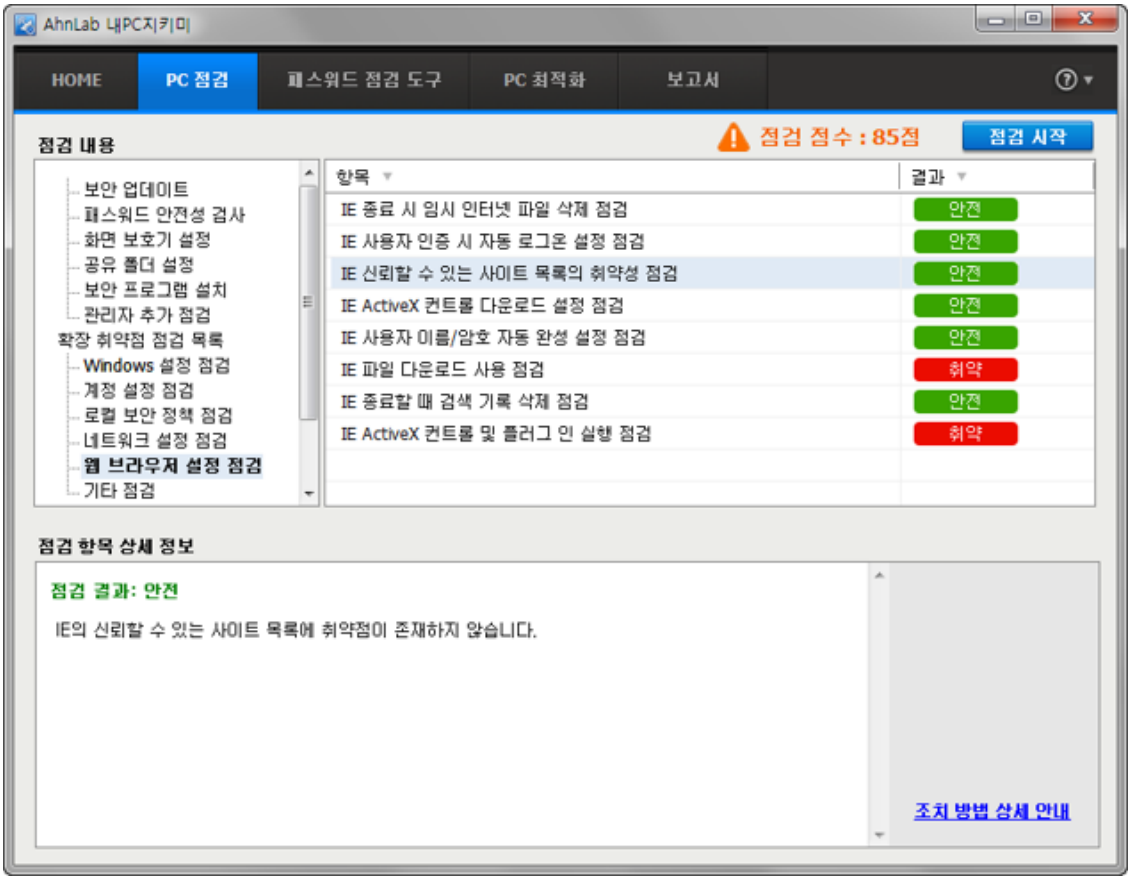
IE 신뢰할 수 있는 사이트 목록의 취약성 점검

사용자 PC 의 IE 신뢰할 수 있는 사이트 목록에 취약성이 존재하는지 점검합니다. 관리자가 신뢰할 수 없는 사이트로 등록한 정보가 사용자 PC 에서는 신뢰할 수 있는 사이트로 등록되어 있는 지 점검합니다.

점검 방법

IE 신뢰할 수 있는 사이트 목록의 취약성 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 **IE 신뢰할 수 있는 사이트 목록의 취약성 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: IE 의 신뢰할 수 있는 사이트 목록에 취약점이 존재하지 않습니다.
   - 취약: IE 의 신뢰할 수 있는 사이트 목록에 신뢰할 수 없는 사이트 URL 이 추가되어 있습니다. **원클릭 조치**를 눌러 신뢰할 수 없는 사이트 URL 을 삭제하십시오.

조치 방법

- IE 신뢰할 수 있는 사이트 목록의 취약성 점검

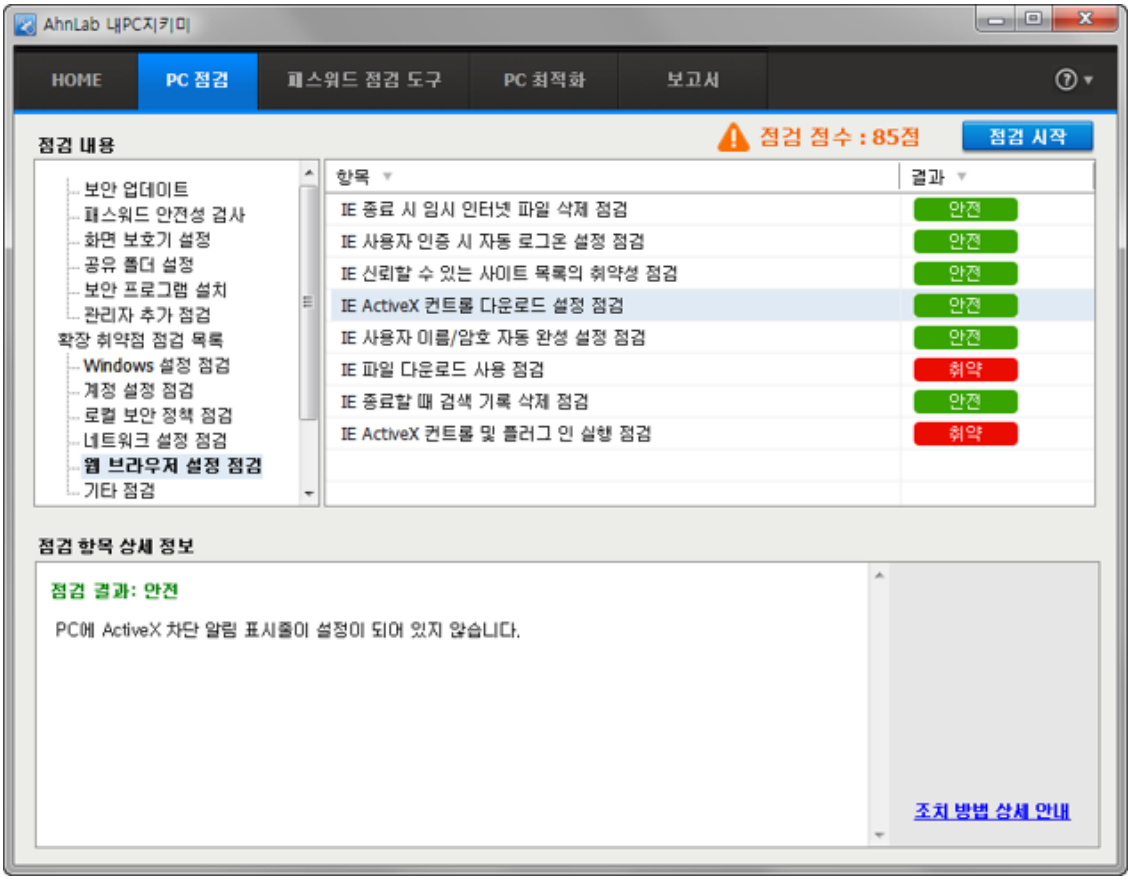
IE ActiveX 컨트롤 다운로드 설정 점검

IE 의 ActiveX 컨트롤 다운로드 설정을 점검합니다. 서명된/서명 안 된 ActiveX 컨트롤 다운로드를 **사용**하도록 설정되어 있으면 취약으로 진단됩니다.

점검 방법

IE ActiveX 컨트롤 다운로드 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 **IE ActiveX 컨트롤 다운로드 설정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: IE ActiveX 컨트롤 다운로드 설정이 안전하게 설정되어 있습니다. **서명된/서명 안 된 ActiveX 컨트롤 다운로드** 설정이 **사용(안전하지 않음)**으로 설정되어 있지 않습니다.
   - 취약: IE ActiveX 컨트롤 다운로드 설정이 안전하지 않도록 설정되어 있습니다. **서명된/서명 안 된 ActiveX 컨트롤 다운로드** 설정이 하나라도 **사용(안전하지 않음)**으로 되어 있으면 취약으로 진단됩니다. **원클릭 조치**를 눌러 IE 의 **서명된/서명 안 된 ActiveX 컨트롤 다운로드** 설정을 **확인**으로 설정하십시오.

조치 방법

- IE ActiveX 컨트롤 다운로드 설정 점검

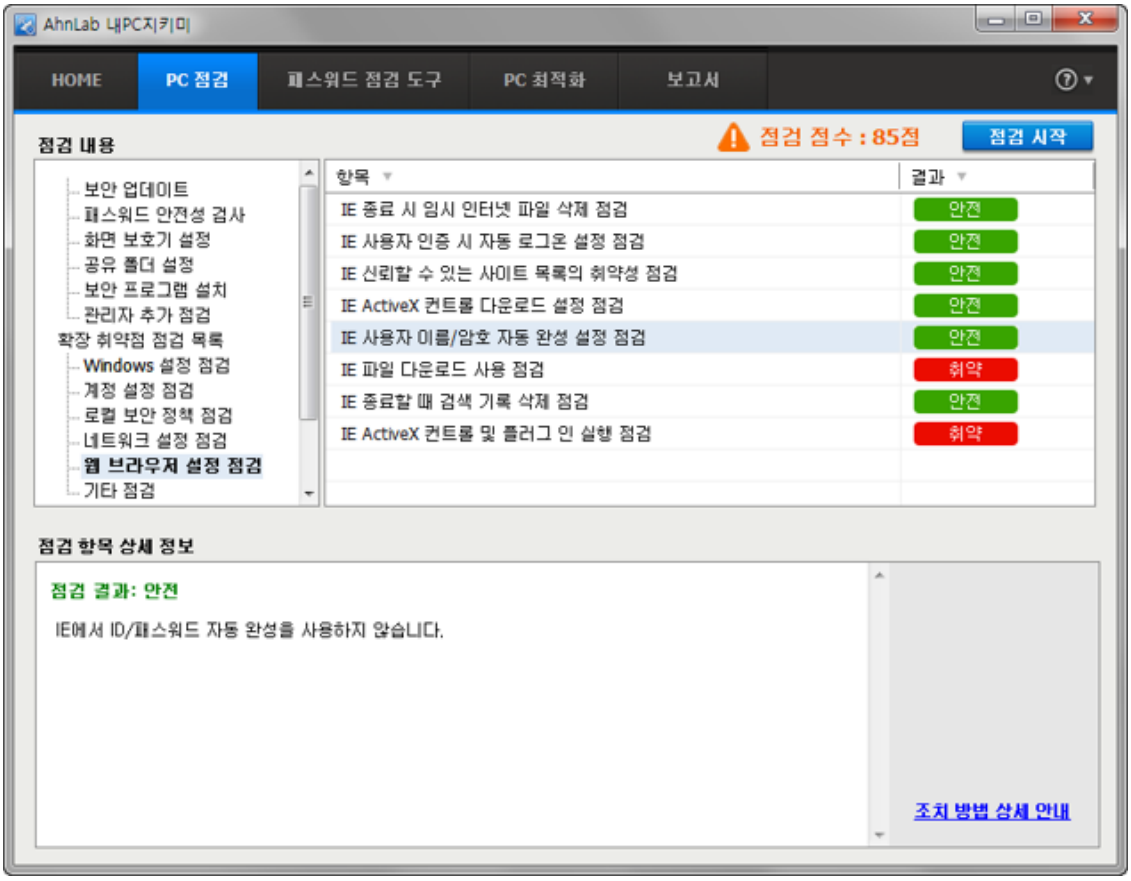
IE 사용자 이름/암호 자동 완성 설정 점검

IE 에서 사용자의 이름과 패스워드 양식을 저장하여 자동 완성되도록 설정되어 있는지 점검합니다.

점검 방법

IE 사용자 이름/암호 자동 완성 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 **IE 사용자 이름/암호 자동 완성 설정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: IE 에서 사용자 이름/암호 자동 완성 기능을 사용하지 않습니다.
   - 취약: IE 에서 사용자 이름/암호 자동 완성 기능을 사용하고 있습니다. **원클릭 조치**를 눌러 사용자 이름/암호 자동 완성 기능을 해제하십시오.

조치 방법

- IE 사용자 이름/암호 자동 완성 설정 점검

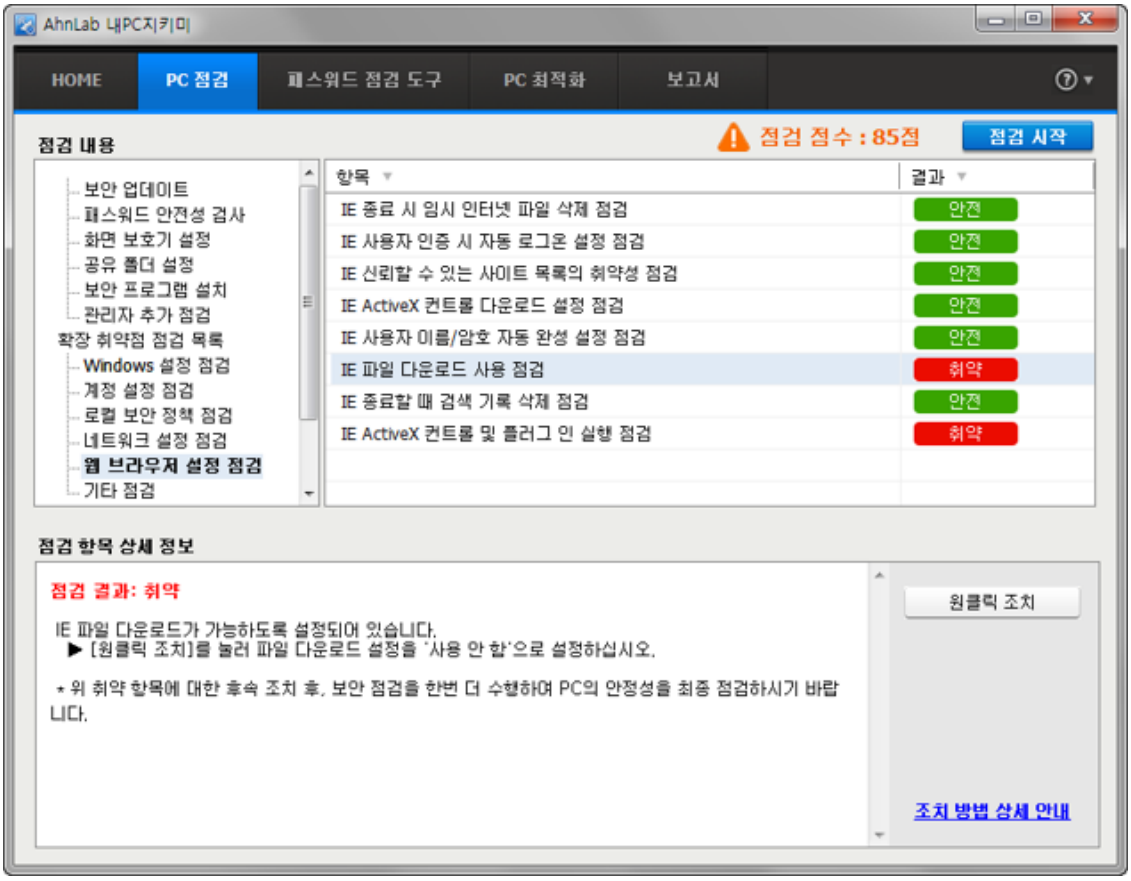
IE 파일 다운로드 사용 점검

IE 에서 파일 다운로드가 가능하도록 설정되어 있는지 점검합니다.

점검 방법

IE 파일 다운로드 사용 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 **IE 파일 다운로드 사용 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: IE 에서 파일 다운로드 설정이 **사용 안 함**으로 설정되어 있습니다.
   - 취약: IE 에서 파일 다운로드 설정이 **사용**으로 설정되어 있습니다. 취약으로 판단된 경우, **원클릭 조치**를 눌러 해당 기능을 **사용 안 함**으로 설정해야 합니다.

조치 방법

- IE 파일 다운로드 사용 점검

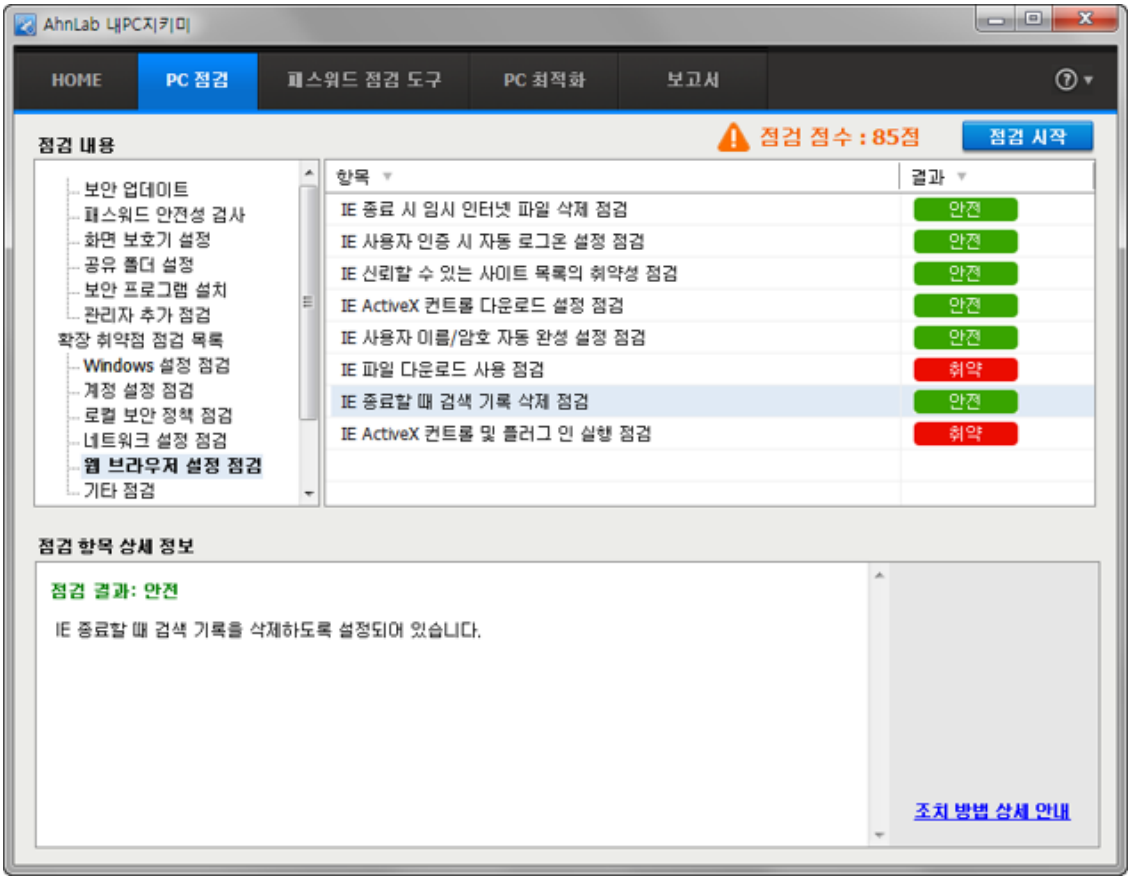
IE 종료할 때 검색 기록 삭제 점검

IE 를 종료할 때 검색 기록을 삭제하도록 설정되어 있는지 점검합니다.

점검 방법

IE 종료할 때 검색 기록 삭제 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내PC지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 **IE 종료할 때 검색 기록 삭제 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: IE 검색 기록 설정에서 **종료할 때 검색 기록 삭제**가 선택되어 있습니다.
   - 취약: IE 검색 기록 설정에서 **종료할 때 검색 기록 삭제**가 선택 해제되어 있습니다. 점검 결과가 **취약**으로 진단된 경우, **원클릭 조치**를 눌러 해당 기능을 선택하도록 설정해야 합니다.

조치 방법

- IE 종료할 때 검색 기록 삭제 점검

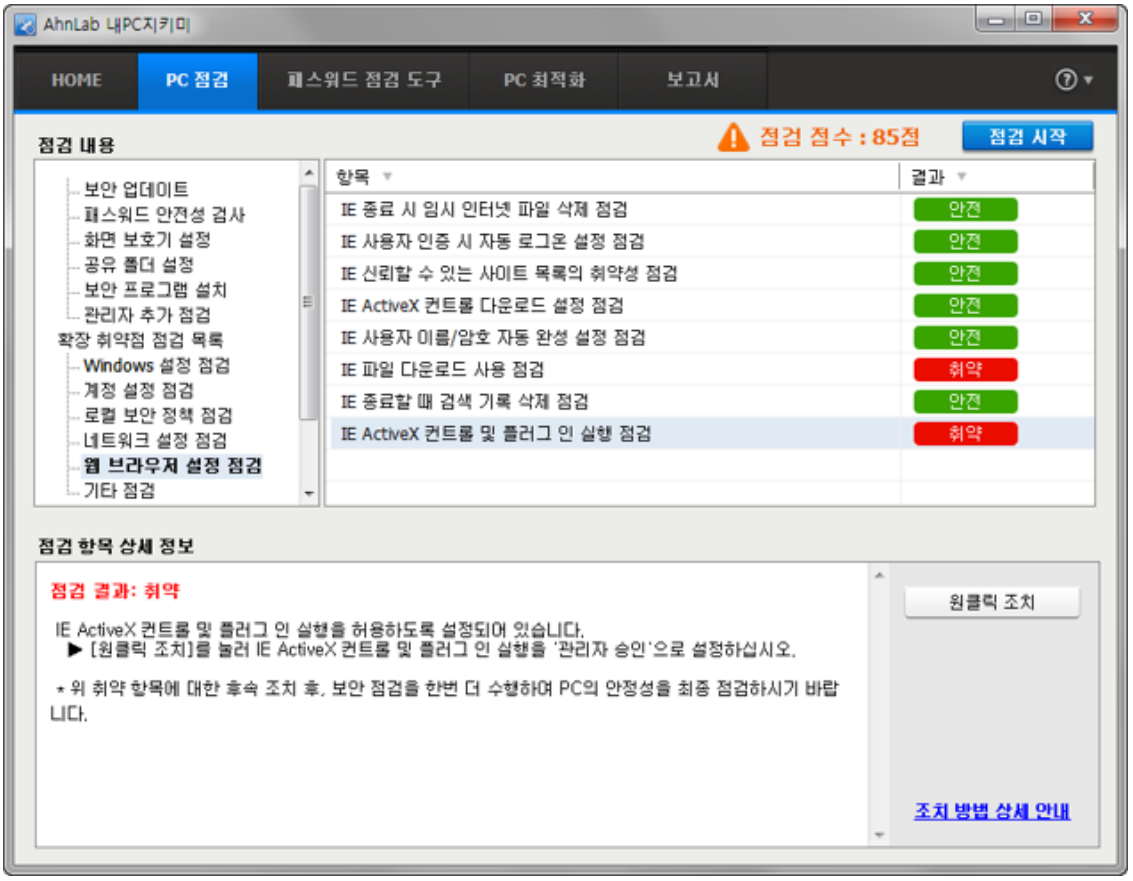
IE ActiveX 컨트롤 및 플러그 인 실행 점검

IE 의 ActiveX 컨트롤 및 플러그 인 실행이 **사용**으로 설정되어 있는지 점검합니다.

점검 방법

IE ActiveX 컨트롤 및 플러그 인 실행 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 **IE ActiveX 컨트롤 및 플러그 인 실행 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: IE ActiveX 컨트롤 및 플러그 인 실행의 설정 값이 **관리자 승인/사용 안 함/확인**으로 설정된 경우입니다.
   - 취약: IE ActiveX 컨트롤 및 플러그 인 실행의 설정 값이 **사용**으로 설정된 경우입니다. 점검 결과가 **취약**으로 진단된 경우, **원클릭 조치**를 눌러 IE 의 ActiveX 컨트롤 및 플러그 인 실행을 **관리자 승인**으로 설정하십시오.

조치 방법

- IE ActiveX 컨트롤 및 플러그 인 실행 점검

기타 점검

NTP 시간 서버와 자동 동기화 설정 점검

사용자 PC 의 시간이 NTP 시간 서버와 자동 동기화하도록 설정되어 있는지 점검하여 결과를 알려줍니다.

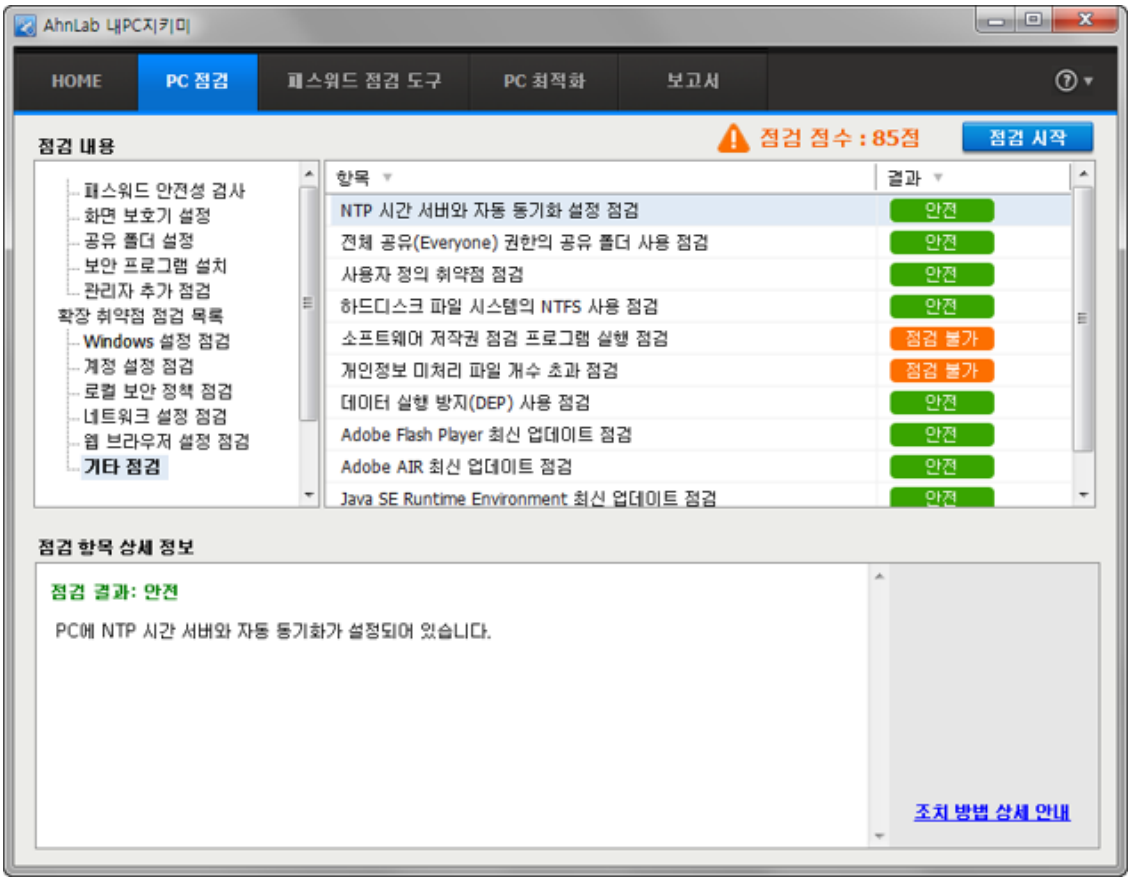
NTP 시간 서버와 동기화

NTP 시간 서버와 동기화란 사용자 PC 의 시간을 NTP(Network Time Protocol) 서버와 동기화하는 것을 의미합니다. 즉, 사용자 PC 의 시간을 NTP 시간 서버의 시간과 일치하도록 업데이트하여 사용자 PC 의 시간을 정확하게 유지할 수 있습니다. 시간은 일반적으로 일주일에 한 번 업데이트 되며, 동기화를 수행하기 위해서는 인터넷에 연결해야 합니다. NTP 시간 서버와 자동 동기화 설정 여부를 점검하는 방법은 다음과 같습니다.

점검 방법

NTP 시간 서버와 자동 동기화 설정 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 기타 점검에서 **NTP 시간 서버와 자동 동기화 설정 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 사용자 PC 가 NTP 시간 서버와 자동으로 동기화되도록 설정되어 있습니다.

- 취약: 사용자 PC 가 NTP 시간 서버와 자동으로 동기화되도록 설정되지 않은 경우입니다. 취약으로 진단된 경우, **원클릭 조치**를 눌러 사용자 PC 의 시간이 NTP 시간 서버와 동기화되도록 설정해야 합니다.

조치 방법

- NTP 시간 서버와 자동 동기화 설정 점검

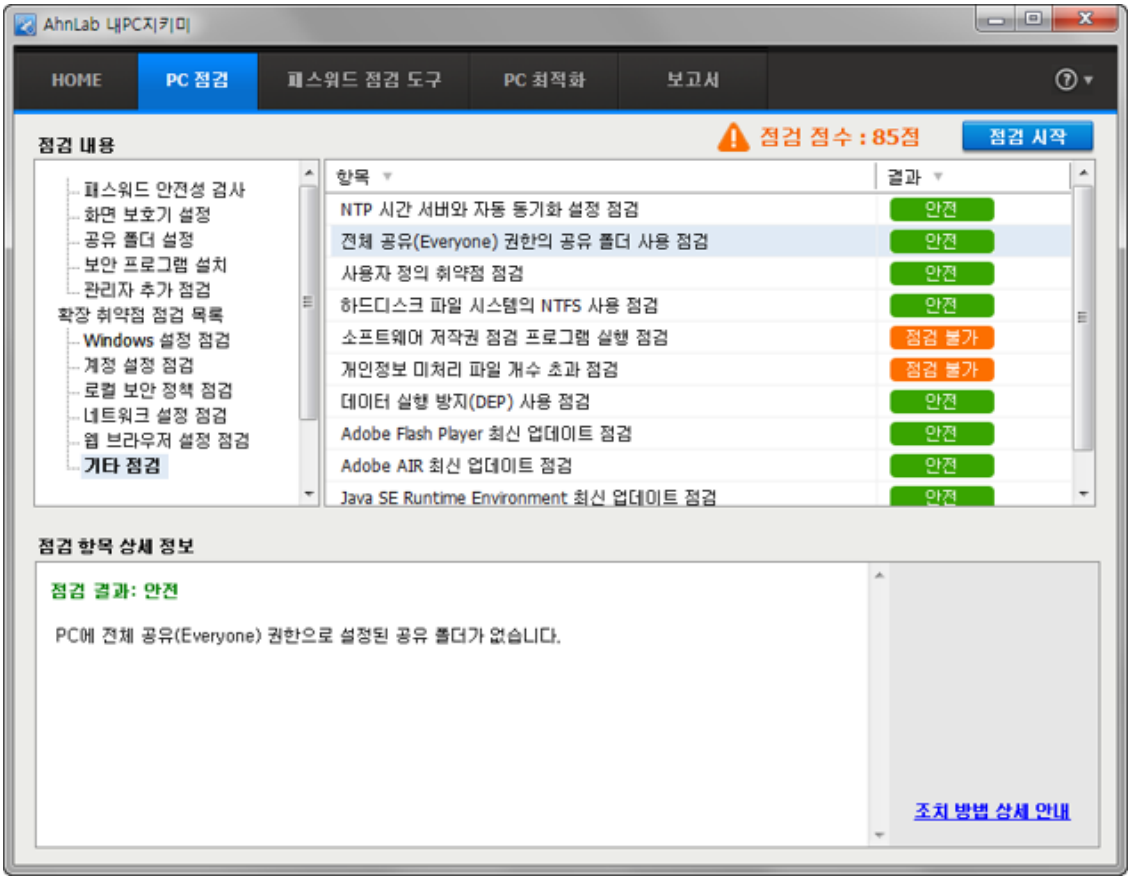
전체 공유(Everyone) 권한의 공유 폴더 사용 점검

사용자 PC 에 전체 공유로 쓰이는 공유 폴더가 사용 중인지 점검하여 결과를 알려줍니다.

점검 방법

전체 공유(Everyone) 권한의 공유 폴더 사용 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 기타 점검에서 **전체 공유로 쓰이는 공유 폴더 사용 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 전체 공유로 쓰이는 공유 폴더를 사용하고 있지 않은 경우입니다.
   - 취약: 전체 공유로 쓰이는 공유 폴더를 사용 중인 경우입니다. 취약으로 진단된 경우, **공유 폴더 해제하기**를 눌러 PC 에 설정되어 있는 모든 사용자 공유 폴더를 해제하십시오.

조치 방법

- 전체 공유(Everyone) 권한의 공유 폴더 사용 점검

사용자 정의 취약점 점검

사용자 정의 취약점 점검 항목들이 안전 조건을 준수하고 있는지 점검하여 결과를 알려줍니다.

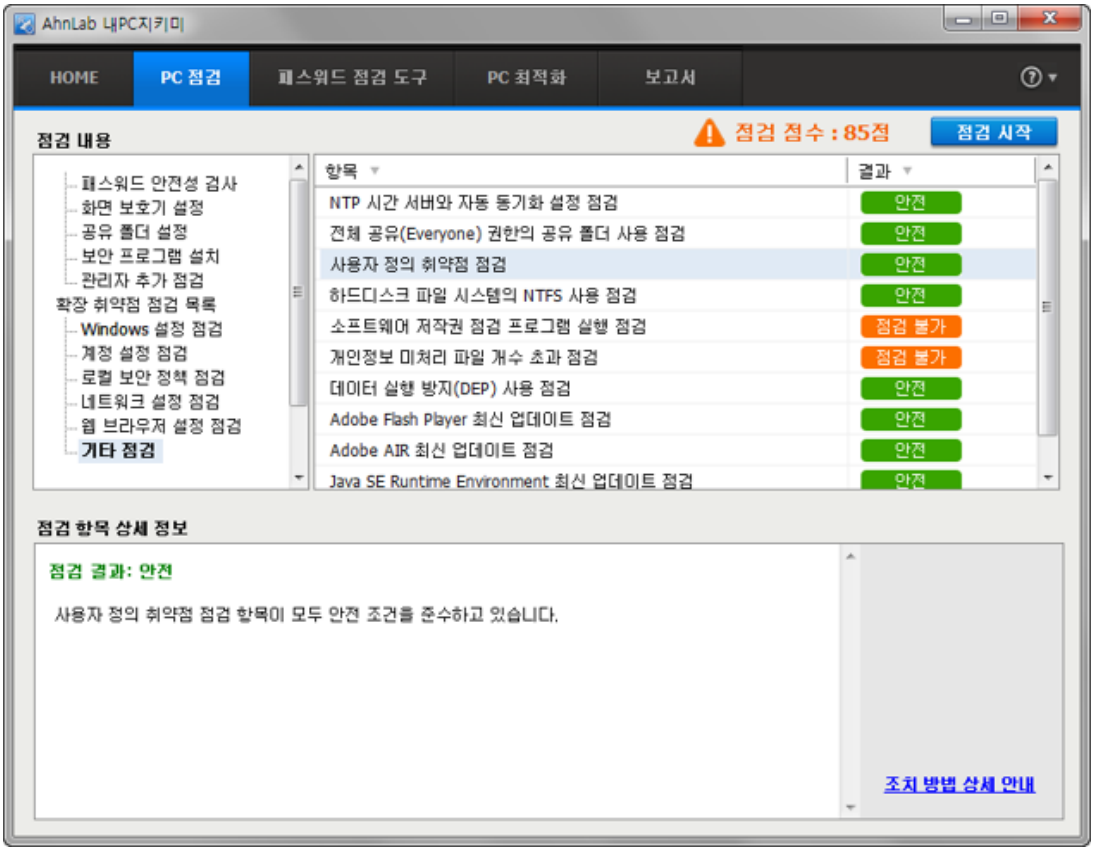
사용자 정의 취약점 점검

- 사용자 정의 취약점 점검은 관리자가 미리 지정한 취약점 점검 조건을 준수하고 있는지 점검
- 점검 항목은 프로세스, 서비스, 레지스트리 경로, 레지스트리 키, 파일 경로, 파일 버전
- 관리자는 4 가지의 점검 항목에 대해 각각 **안전 조건(실행/중지 여부, 경로 있음/없음 여부)**을 설정가능

점검 방법

사용자 정의 취약점 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 기타 점검에서 사용자 정의 취약점 점검을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 사용자 정의 취약점 점검 항목이 모두 안전 조건을 준수하고 있습니다.
   - 취약: 사용자 정의 점검 항목들이 안전 조건을 준수하고 있지 않은 경우입니다. 취약으로 진단된 경우 **취약점 해결하기**를 눌러 안전 조건에 따라 취약 서비스의 상태를 변경하십시오. 또는 **점검 항목 상세 정보**에 명시되어 있는 **안전 조건**을 준수하여, 취약 항목에 대한 조치를 취하십시오.

조치 방법

- 사용자 정의 취약점 점검

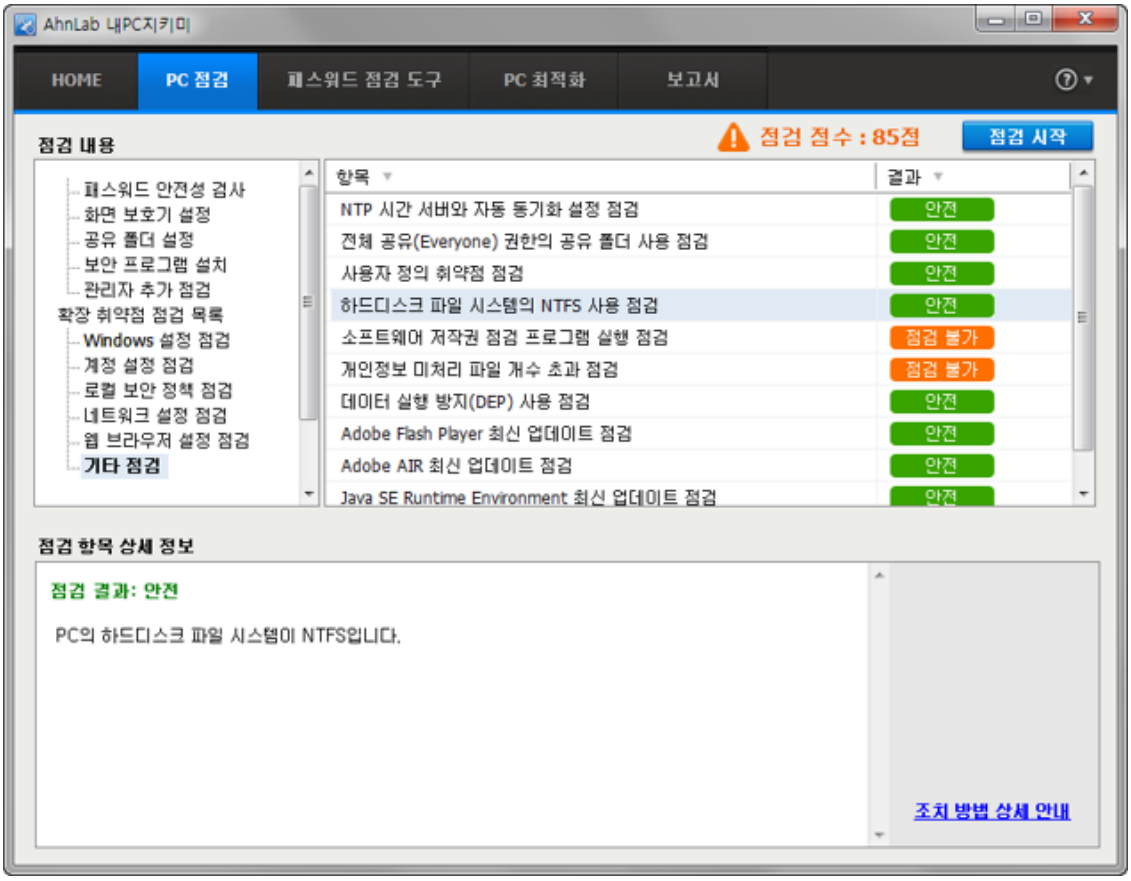
하드디스크 파일 시스템의 NTFS 사용 점검

사용자 PC 에 하드디스크 파일 시스템이 NTFS 를 사용하도록 설정되어 있는지 점검하여 결과를 알려줍니다.

점검 방법

하드디스크 파일 시스템의 NTFS 사용 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 기타 점검에서 **하드디스크 파일 시스템의 NTFS 사용 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: PC 의 하드디스크 파일 시스템이 NTFS 입니다.
   - 취약: PC 에 하드디스크의 파일 시스템이 NTFS 를 사용하도록 설정되어 있지 않습니다. **원클릭 조치**를 눌러 하드디스크 파일 시스템이 NTFS 를 사용하도록 설정하십시오.

조치 방법

- 하드디스크 파일 시스템의 NTFS 사용 점검

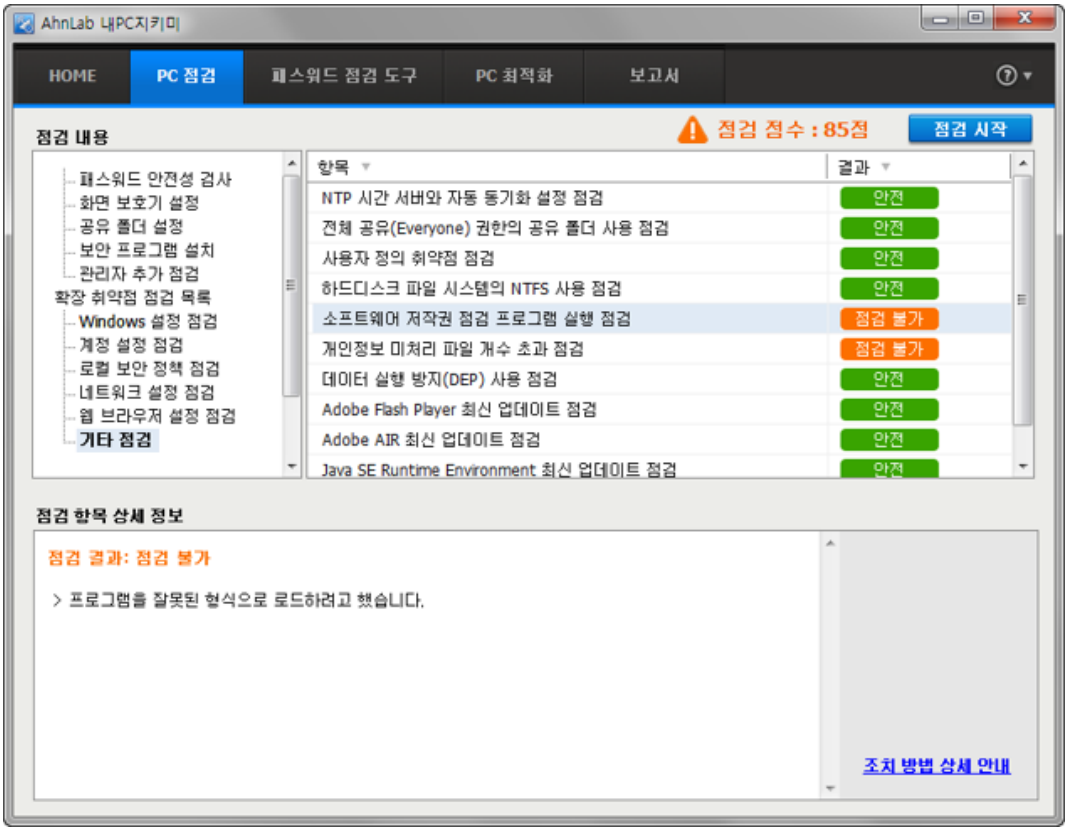
소프트웨어 저작권 점검 프로그램 실행 점검

사용자 PC 의 소프트웨어 저작권 점검 프로그램이 관리자가 설정한 조건 내에 실행되었는지 점검합니다.

점검 방법

소프트웨어 저작권 점검 프로그램 실행 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 확장 취약점 점검 목록 > 기타 점검에서 **소프트웨어 저작권 점검 프로그램 실행 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 소프트웨어 저작권 점검 프로그램이 관리자가 설정한 안전 조건 내에 실행되었습니다.
   - 취약: 소프트웨어 저작권 점검을 수행하지 않았거나, 관리자가 설정한 기간 내에 소프트웨어 저작권 점검을 수행하지 않은 경우입니다. 취약으로 판단된 경우, **프로그램 실행하기**를 눌러 AhnLab Patch Management 프로그램에서 소프트웨어 저작권 점검을 수행하십시오.
   - 점검 불가: 소프트웨어 저작권 점검 프로그램 실행 여부를 확인할 수 없는 경우입니다. 관련 제품의 라이선스를 확인하십시오.

참고

AhnLab Patch Management 라이선스가 없는 경우에는 점검을 수행할 수 없습니다. 해당 항목을 점검하려면 관련 제품의 라이선스를 구입해야 합니다.

조치 방법

- 소프트웨어 저작권 점검 프로그램 실행 점검

개인 정보 미처리 파일 개수 초과 점검

사용자 PC 에 처리되지 않은 개인정보 보유 파일이 안전 조건을 초과하여 존재하는지 점검하여 결과를 알려줍니다.

개인 정보 미처리 파일

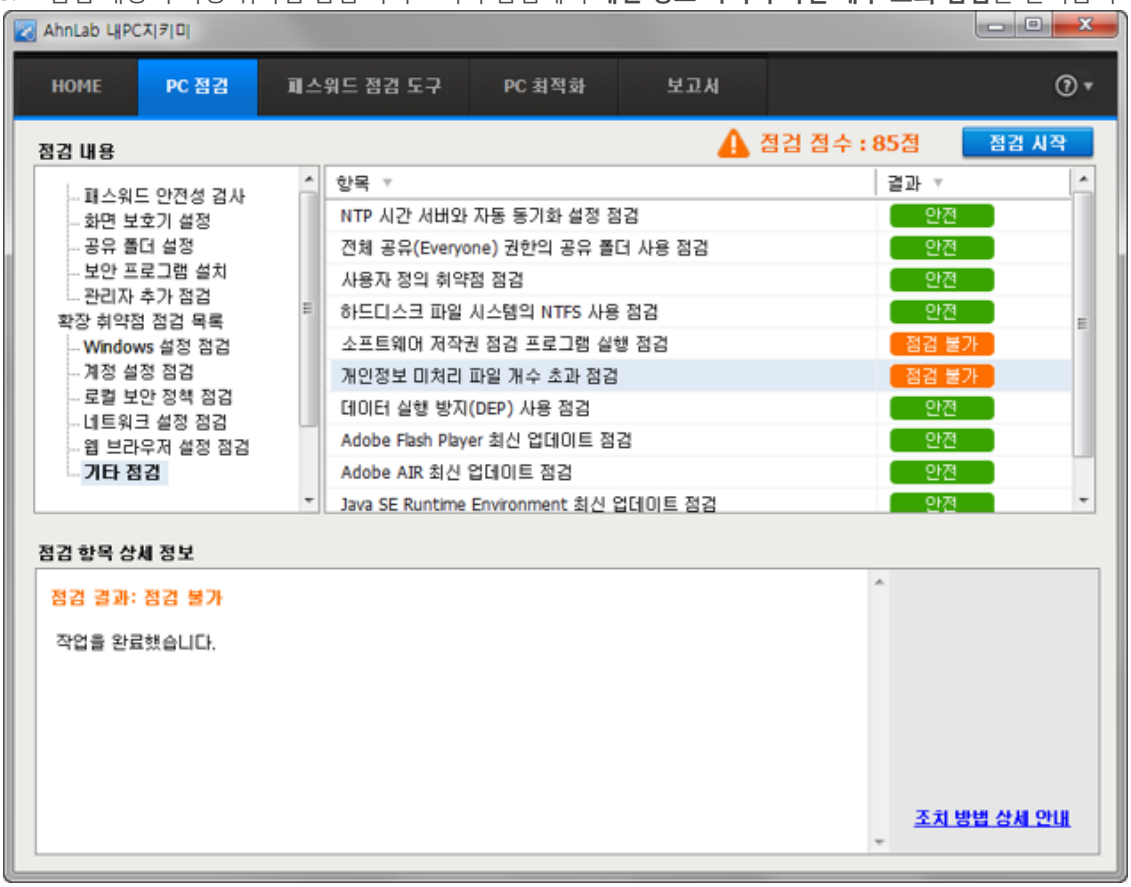
개인 정보를 보유하고 있는 파일이지만, 아무런 조치를 취하지 않은 파일을 **개인 정보 미처리 파일**로 분류합니다. 사용자 PC 에서 개인 정보를 보유한 파일이 발견되면 해당 파일을 **완전 삭제**해야 하며, 삭제를 보류하기 위해서는 **격리**, **암호화**, **예외** 3 가지의 처리 방법 중 1 가지를 수행해야 합니다.

- 완전 삭제: 개인 정보 보유 파일을 사용자 PC 에서 완전 삭제하여 복구할 수 없도록 합니다.
- 격리: 개인 정보 보유 파일을 격리 공간으로 이동하여 저장합니다.
- 암호화: 개인 정보 보유 파일을 암호화하여 보관합니다.
- 예외 처리: 개인 정보 보유 파일이지만 파일을 격리하거나 암호화하지 않고 사용합니다.

점검 방법

개인 정보 미처리 파일 개수 초과 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 기타 점검에서 **개인 정보 미처리 파일 개수 초과 점검**을 선택합니다.



4. 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**가 표시됩니다.
   - 안전: 처리되지 않은 개인정보 보유 파일의 개수가 안전 조건을 초과하지 않았습니다.

- 취약: 처리되지 않은 개인정보 보유 파일의 개수가 안전 조건을 초과한 경우입니다. 취약으로 진단된 경우, **프로그램 실행하기**를 눌러 AhnLab Privacy Management 프로그램에서 처리되지 않은 개인 정보 파일들을 모두 처리하십시오.

참고

AhnLab Privacy Management 라이선스가 없는 경우에는 점검을 수행할 수 없습니다. 해당 항목을 점검하려면 관련 제품의 라이선스를 구입해야 합니다.

조치 방법

- 개인 정보 미처리 파일 개수 초과 점검

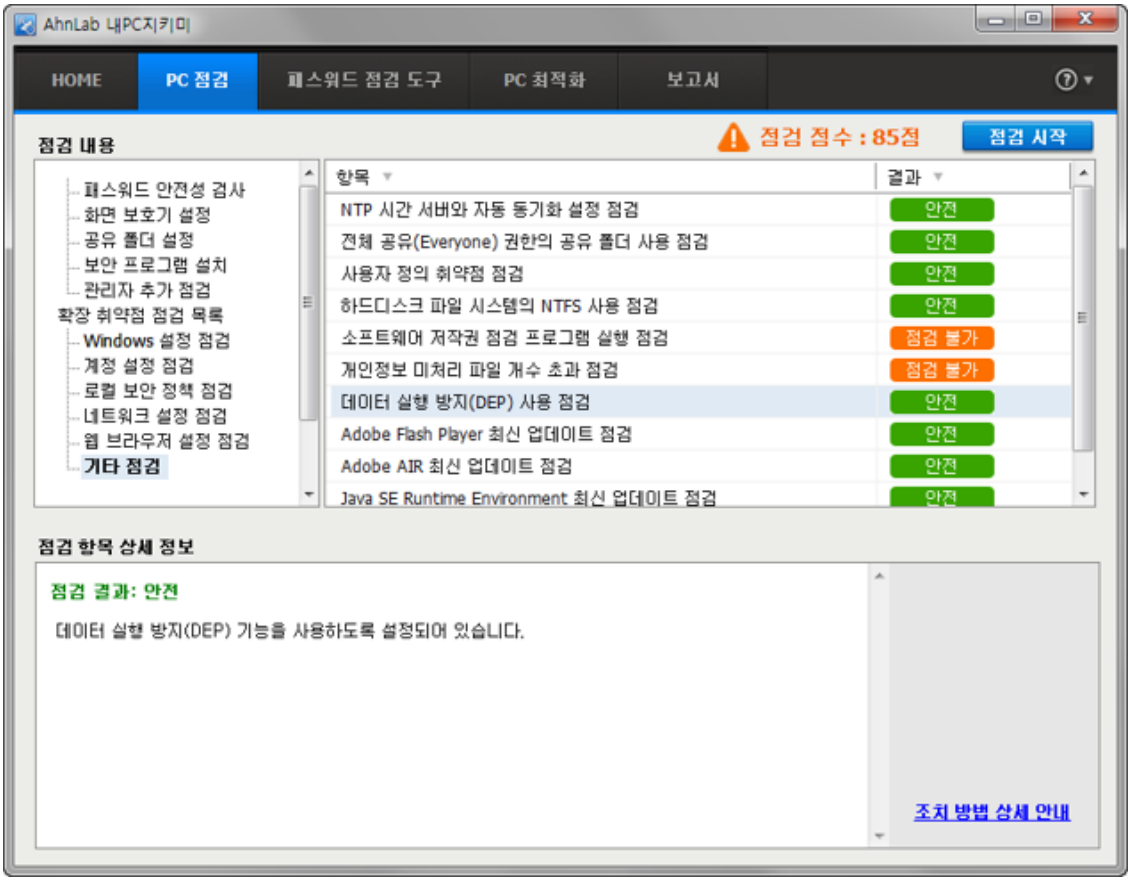
데이터 실행 방지(DEP) 사용 점검

데이터 실행 방지(Data Execution Prevention) 기능을 사용하고 있는지 점검합니다.

점검 방법

데이터 실행 방지(DEP) 사용 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 기타 점검에서 데이터 실행 방지(DEP) 사용 **점검**을 선택합니다.



4. 데이터 실행 방지(DEP) 사용 점검 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**에 점검 결과가 표시됩니다.
   - 안전: 데이터 실행 방지(DEP)기능을 사용하고 있습니다.
   - 취약: 데이터 실행 방지(DEP) 기능을 사용하지 않고 있습니다. **원클릭 조치**를 눌러 데이터 실행 방지(DEP) 기능을 사용하도록 설정하십시오.

조치 방법

- 데이터 실행 방지(DEP) 사용 점검

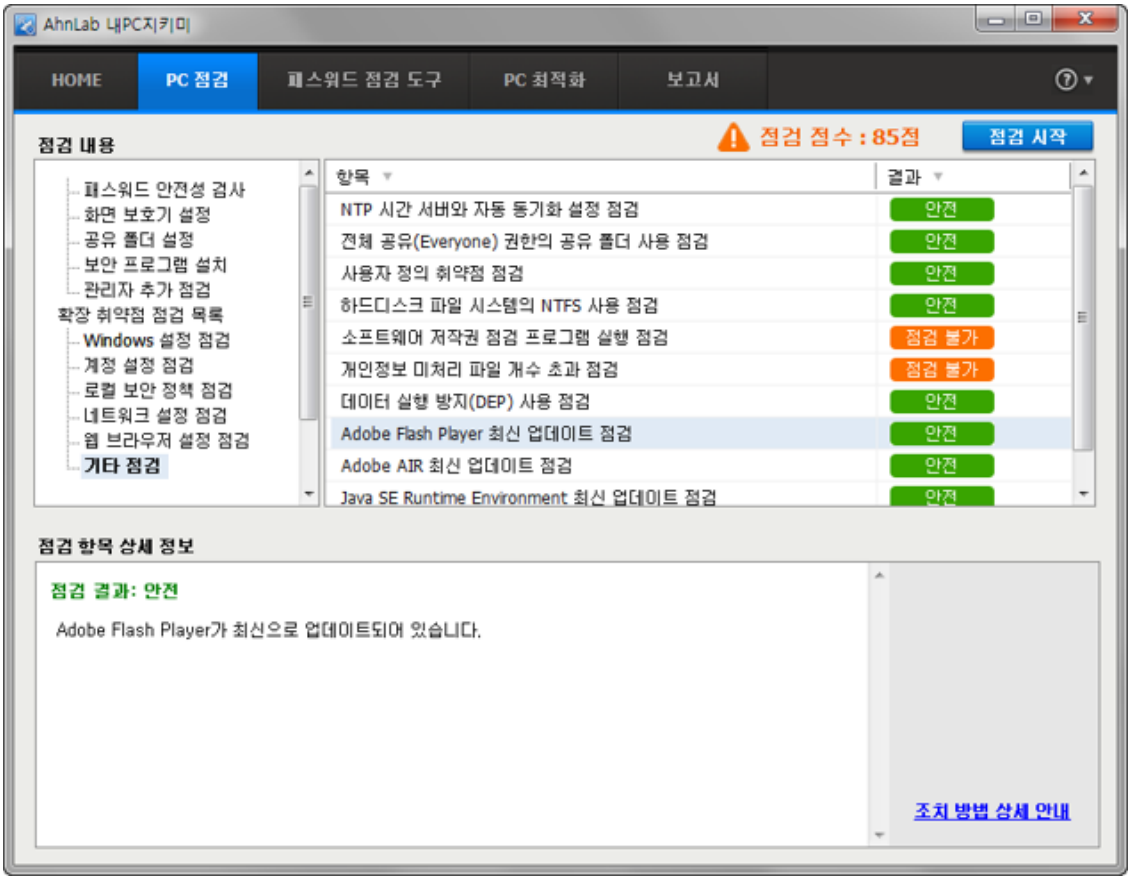
Adobe Flash Player 최신 업데이트 점검

Adobe Flash Player 가 최신으로 업데이트되어 있는지를 점검합니다.

점검 방법

Adobe Flash Player 최신 업데이트 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 기타 점검에서 **Adobe Flash Player 최신 업데이트 점검**을 선택합니다.



4. **Adobe Flash Player 최신 업데이트 점검** 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**에 점검 결과가 표시됩니다.
   - 안전: Adobe Flash Player 가 최신으로 업데이트되어 있습니다.
   - 취약: Adobe Flash Player 가 최신 업데이트 상태가 아닙니다. **업데이트 설치하기**를 눌러 최신 버전으로 업데이트하시기 바랍니다.

조치 방법

- Adobe Flash Player 최신 업데이트 점검

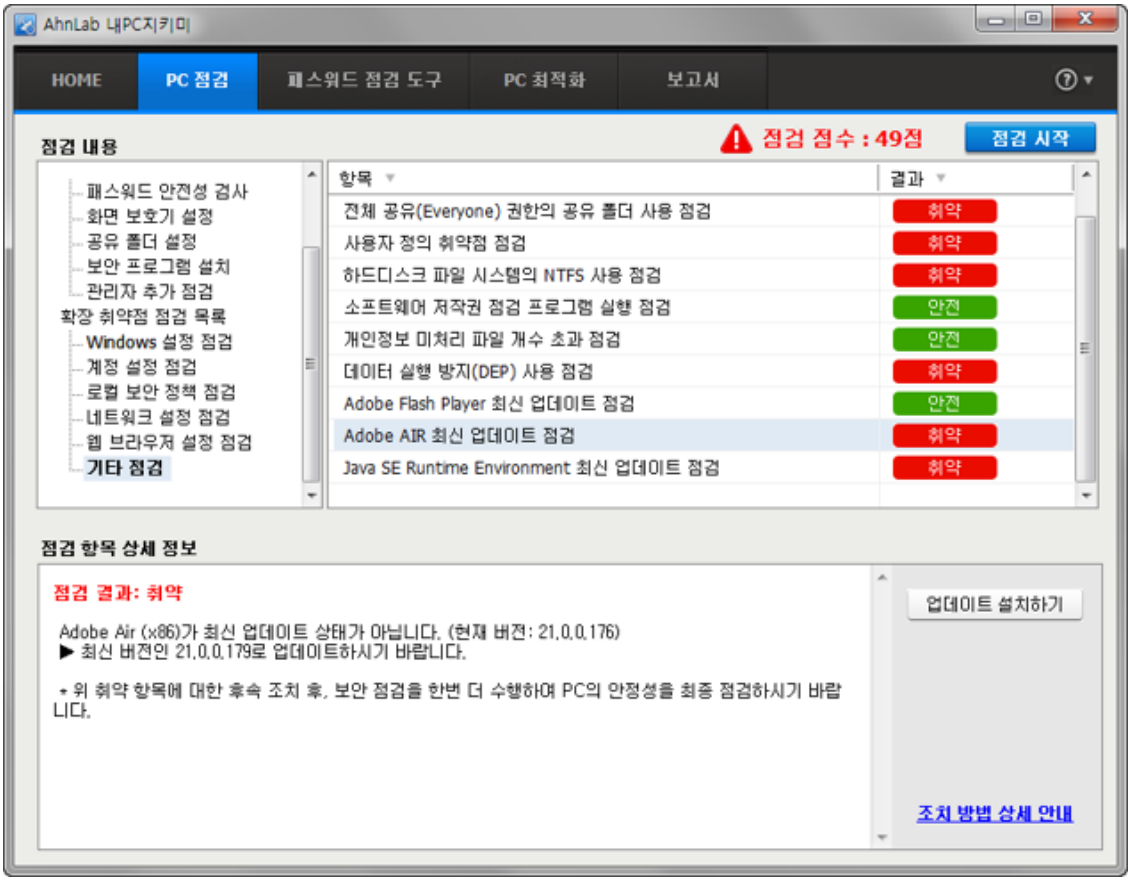
Adobe AIR 최신 업데이트 점검

Adobe AIR 가 최신으로 업데이트되어 있는지를 점검합니다.

점검 방법

Adobe AIR 최신 업데이트 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 기타 점검에서 **Adobe AIR 최신 업데이트 점검**을 선택합니다.



4. **Adobe AIR 최신 업데이트 점검** 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**에 점검 결과가 표시됩니다.
   - 안전: Adobe AIR 가 최신으로 업데이트되어 있습니다.
   - 취약: Adobe AIR 가 최신 업데이트 상태가 아닙니다. **업데이트 설치하기**를 눌러 최신 버전으로 업데이트하시기 바랍니다.

조치 방법

- Adobe AIR 최신 업데이트 점검

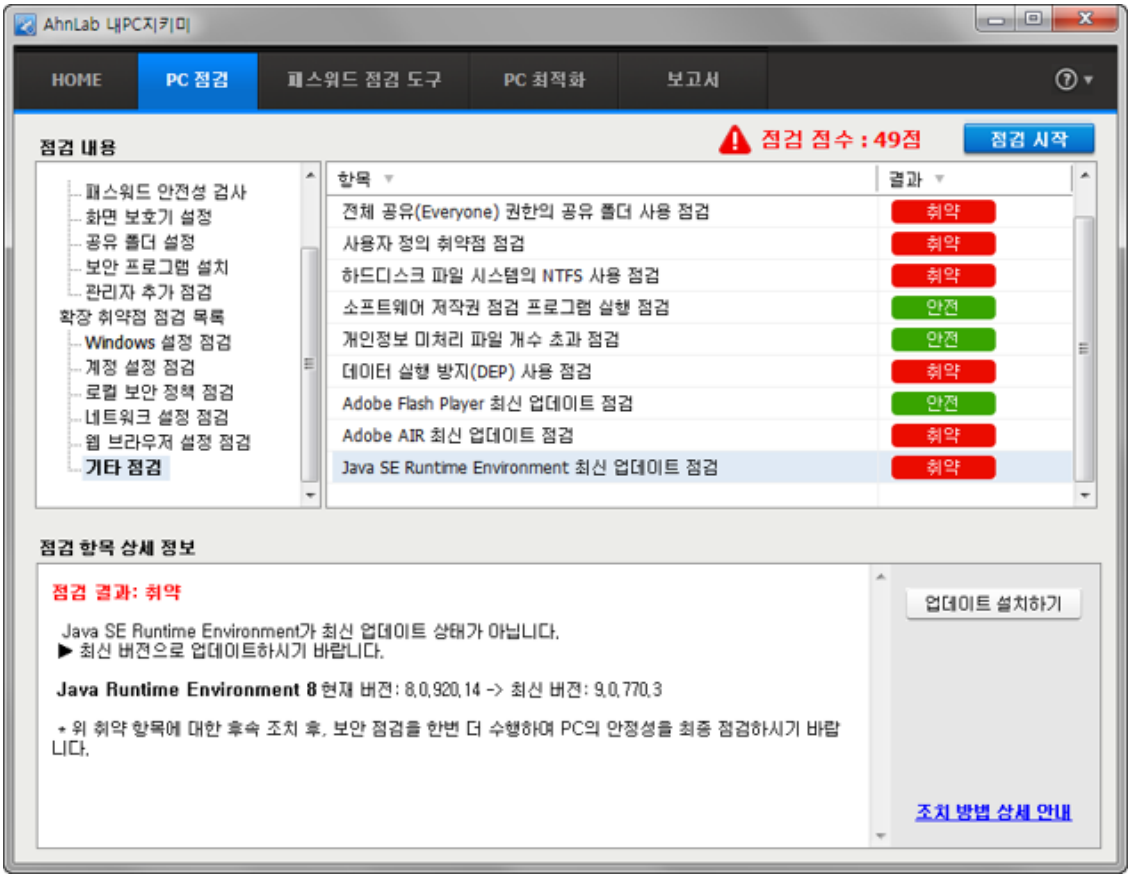
Java SE Runtime Environment 최신 업데이트 점검

Adobe AIR 가 최신으로 업데이트되어 있는지를 점검합니다.

점검 방법

Java SE Runtime Environment 최신 업데이트 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 기타 점검에서 **Java SE Runtime Environment 최신 업데이트 점검**을 선택합니다.



4. **Java SE Runtime Environment 최신 업데이트 점검** 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**에 점검 결과가 표시됩니다.
   - 안전: Java SE Runtime Environment 가 최신으로 업데이트되어 있습니다.
   - 취약: Java SE Runtime Environment 가 최신 업데이트 상태가 아닙니다. **업데이트 설치하기**를 눌러 최신 버전으로 업데이트하시기 바랍니다.

조치 방법

- Java SE Runtime Environment 최신 업데이트 점검

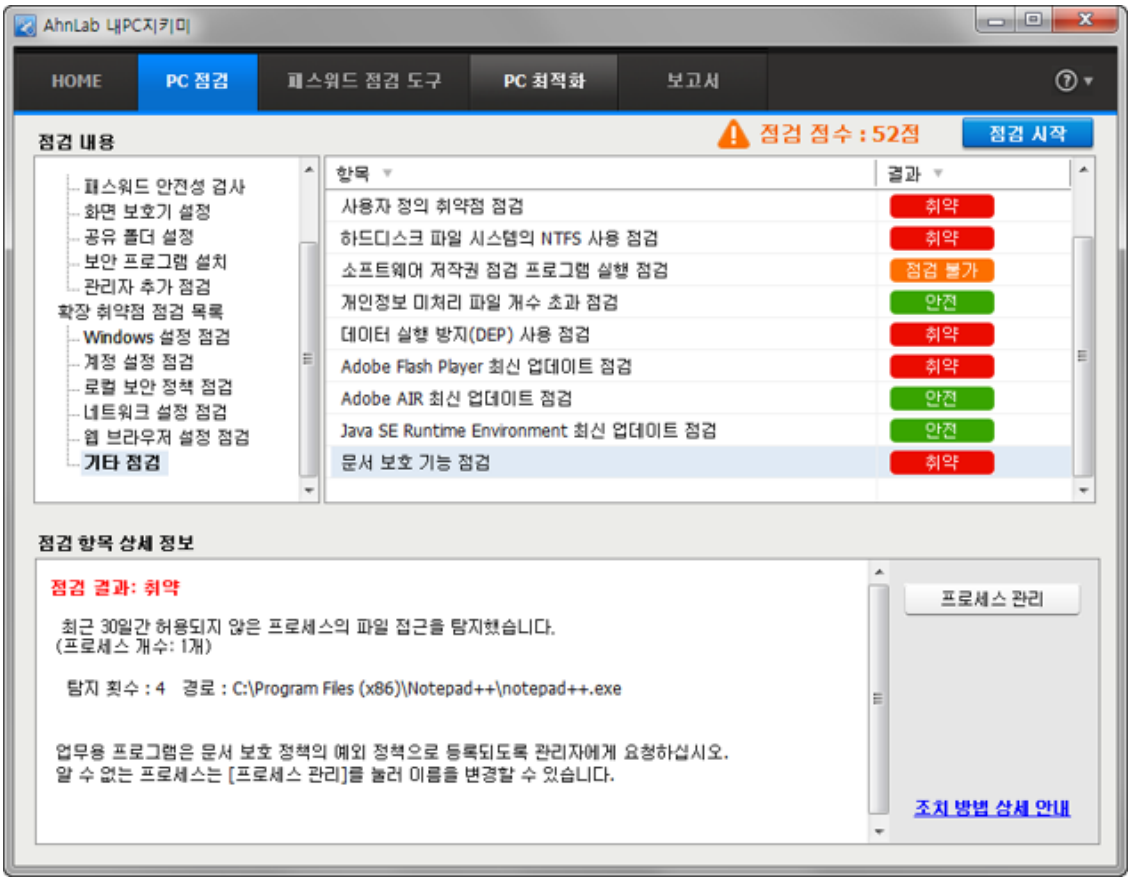
문서 보호 기능 점검

특정 문서 확장자(doc, docx, ...)를 가진 파일에 대해 허용된 프로세스만 접근을 허용하고, 나머지 프로세스는 모두 접근을 차단하여 문서를 보호하는 기능 입니다. 문서 보호 기능 점검은 관리 콘솔에서 **문서 보호 기능**을 사용하도록 설정해야만 점검 항목으로 나타납니다.

점검 방법

문서 보호 기능 점검 방법은 다음과 같습니다.

1. 보안 점검을 실행하여 점검 결과를 확인합니다.
2. 점검 완료 창을 닫은 후 내 PC 지키미의 **PC 점검** 탭을 선택합니다.
3. 점검 내용의 확장 취약점 점검 목록 > 기타 점검에서 **문서 보호 기능 점검**을 선택합니다.



4. **문서 보호 기능 점검** 항목을 선택하면 화면 아래에 **점검 항목 상세 정보**에 점검 결과가 표시됩니다.
   - 안전: 허용되지 않은 프로세스의 접근 기록이 없습니다.
   - 취약: 최근 몇 일 동안 허용되지 않은 프로세스가 파일에 접근하는 것을 탐지했습니다. 업무용 프로그램은 문서 보호 정책의 예외 정책으로 등록되도록 관리자에게 요청하십시오. 알 수 없는 프로세스는 **프로세스 관리**를 눌러 이름을 변경할 수 있습니다.

조치 방법

- 문서 보호 기능 점검

5 장

패스워드 점검 도구

패스워드 점검

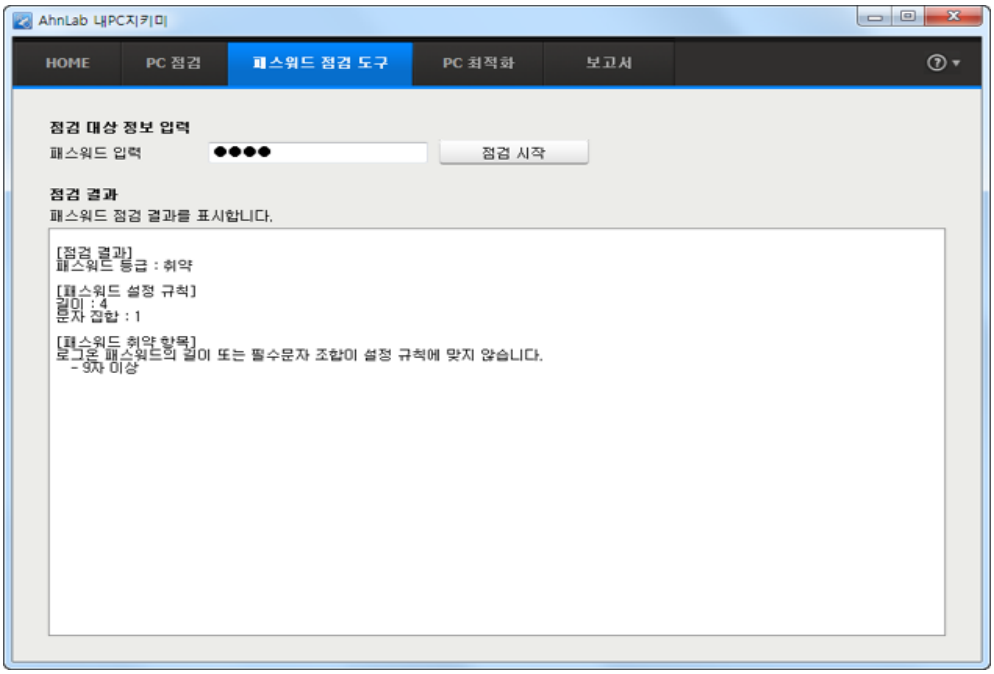
패스워드 점검

패스워드 점검에서는 사용자가 입력한 패스워드의 안전성을 점검합니다. 패스워드 점검은 패스워드의 길이, 연속한 단어나 숫자의 포함 여부, 많이 사용하는 단어의 포함 여부 등을 점검합니다.

점검 방법

패스워드 점검 방법은 다음과 같습니다.

1. 바탕 화면에 있는 내 PC 지키미 아이콘을 더블 클릭합니다.
2. 내 PC 지키미 화면이 나타나면 **패스워드 점검 도구** 탭을 선택합니다.
3. **패스워드 점검 도구** 탭에서 **패스워드 입력**란에 점검 대상 패스워드를 입력하고 **점검 시작**을 누릅니다.



4. 점검 결과 영역에 나타난 점검 결과를 확인합니다.
   - 점검 결과: 관리자가 설정한 정책으로 패스워드 점검 결과를 안전 또는 취약으로 표시합니다.
   - 패스워드 설정 규칙: 패스워드의 길이, 연속된 문자 포함 여부를 점검합니다.

6 장

PC 최적화

PC 최적화

PC 최적화

PC 에 저장된 Windows 임시 파일이나 인터넷 임시 파일 등을 삭제하여 PC 를 최적화합니다.

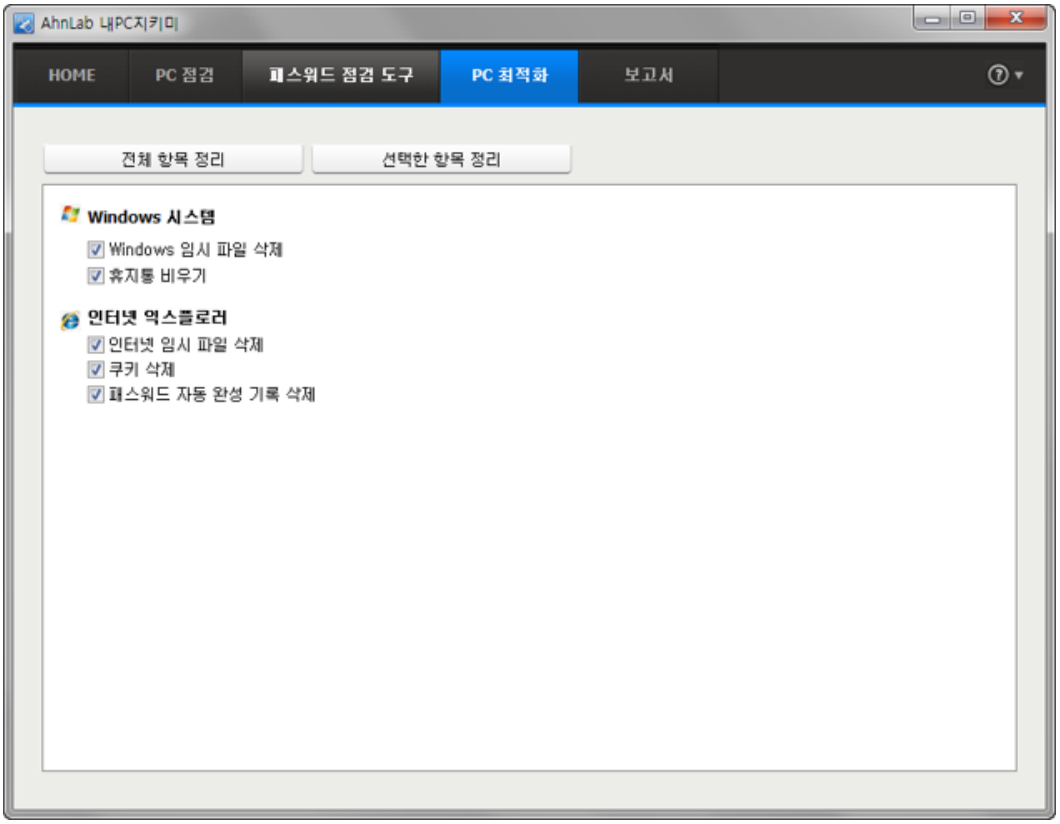
최적화 항목

- **Windows 시스템**
  - Windows 임시 파일 삭제: Windows 시스템에서 최근 사용한 파일을 모두 지웁니다.
  - 휴지통 비우기: 휴지통에 보관된 삭제 파일이나 폴더를 모두 지웁니다.
- **인터넷 익스플로러**
  - 인터넷 임시 파일 삭제: Microsoft Internet Explorer 사용 시에 다운로드 되어 Temporary Internet Files 폴더에 저장된 임시 인터넷 파일을 삭제합니다.
  - 쿠키 삭제: 사용자의 웹사이트 사용 내용을 저장한 쿠키를 삭제합니다.
  - 패스워드 자동 완성 기록 삭제: 웹 사이트에서 입력한 비밀번호를 저장해둔 기록인 암호 자동 완성 기록을 삭제합니다.

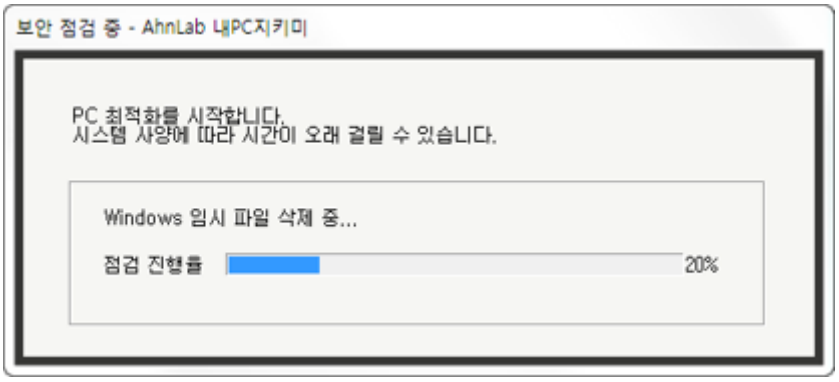
최적화 방법

PC 최적화 방법은 다음과 같습니다.

1. 바탕 화면의 내PC지키미 아이콘을 더블 클릭합니다.
2. 내PC지키미 화면이 나타나면, **PC 최적화** 탭을 선택합니다.
3. **PC 최적화** 화면에서 정리할 항목을 선택합니다.



4. PC 최적화 진행 과정이 화면에 표시됩니다. PC 최적화가 완료되면 진행 화면이 사라집니다.



7 장

보고서

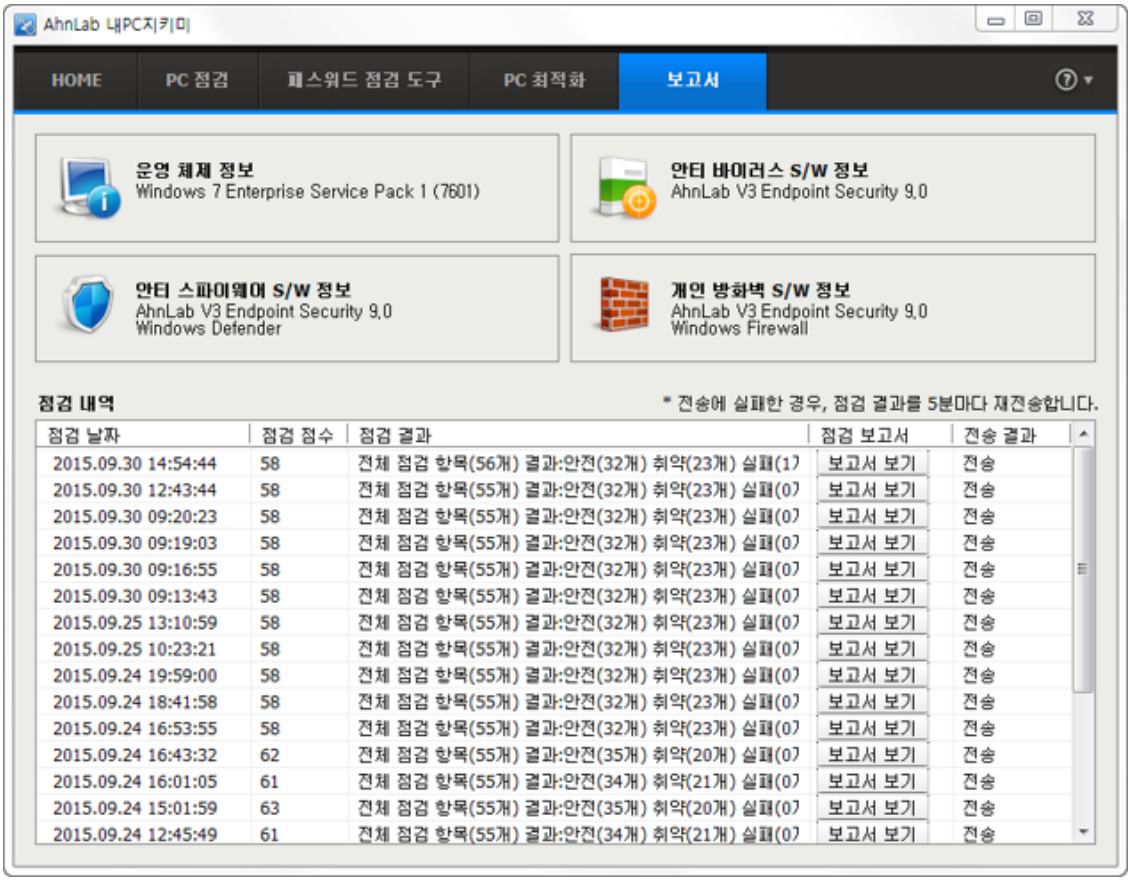
보고서

보고서

보고서를 선택하면, 보안 점검 실행 내역과 사용자 PC 의 운영 체제 정보, 보안 프로그램 설치 정보 등을 확인할 수 있습니다. 보고서 내용은 보안 점검을 완료하면 자동으로 서버 관리자에게 보내집니다.

보고서 구성

보고서는 다음과 같이 사용자 시스템 정보와 점검 결과로 구성되어 있습니다.



사용자 시스템 정보

- 운영 체제 정보: 사용자 PC 에 설치되어 있는 운영 체제의 이름과 버전 정보를 표시합니다.
- 안티 바이러스 S/W 정보: 사용자 PC 에 설치되어 있는 바이러스 백신 프로그램의 이름과 버전 정보를 표시합니다.
- 안티 스파이웨어 S/W 정보: 사용자 PC 에 설치되어 있는 스파이웨어 프로그램의 이름과 버전 정보를 표시합니다.
- 개인 방화벽 S/W 정보: 사용자 PC 에 설치되어 있는 개인 방화벽 프로그램의 이름과 버전 정보를 표시합니다.

점검 내역

- 점검 날짜: 내 PC 지키미 검사를 실행한 날짜와 시간입니다.
- 점검 점수: 내 PC 지키미 검사를 수행한 결과 점수를 나타냅니다.

- 점검 결과: 내 PC 지키미 검사 결과를 보여줍니다. 전체 점검 항목의 개수와 안전, 취약, 실패 항목의 개수를 보여줍니다.
- 점검 보고서: 내 PC 지키미 검사 결과를 보고서 형태로 보여줍니다. 보고서 열기를 누르면 IE 를 실행하여 해당 날짜의 점검 내용에 대한 상세 정보를 볼 수 있습니다.
- 전송 결과: 내 PC 지키미 검사 결과가 AhnLab PC 진단 결과 확인 시스템으로 전송되었는지를 표시합니다.
- 내 PC 지키미 점검 결과 하단의 **점검 내용 상세 정보**에서는 점검 결과에 대한 상세 내역을 확인할 수 있습니다.

보고서 보기

내 PC 지키미 보고서는 다음과 같이 **사용자 정보, 내 PC 지키미 점검 결과, 점검 내용 상세 정보**로 구성되어 있습니다.

내PC지키미 보고서

점검 담당: (서명)

사용자 정보

점검 시간	2015.09.30 14:54:44
IP 주소	
사용자 ID	
컴퓨터 이름	
운영 체제 정보	Windows 7 Enterprise Service Pack 1 (7601)
내PC지키미 버전	4.6.4.2
바이러스 백신	AhnLab V3 Endpoint Security 9.0
점검 결과 서버 전송	전송

내PC지키미 점검 결과 점검 점수: 58점

점검 항목	결과
기본 취약점 점검 목록	
바이러스 백신 설치 및 실행 점검	안전
바이러스 백신의 최신 보안 패치 점검	안전
운영 체제, MS Office 최신 보안 패치 점검	안전
로그온 패스워드 사용 기간 점검	안전
로그온 패스워드 안전성 점검	안전
화면 보호기 설정 점검	안전
사용자 공유 폴더 설정 점검	취약
미사용 ActiveX 프로그램 점검	안전
USB 자동 실행 설정 점검	안전
비인가 프로그램 설치 점검	취약
보안 USB 설치 점검	안전
무선 랜카드 설치 점검	안전
편집 프로그램 설치 점검	취약
PDF 프로그램의 최신 보안 패치 점검	안전
확장 취약점 점검 목록	
Administrators 그룹 내 사용자 계정 점검	취약
패스워드 암호화 알고리즘 설정 점검	안전

점검 내용 상세 정보

▸ 000001 바이러스 백신 설치 및 실행 점검

점검 결과: 안전

8 장

점검 결과와 조치 방법

기본 취약점 점검 목록
확장 취약점 점검 목록

기본 취약점 점검 목록

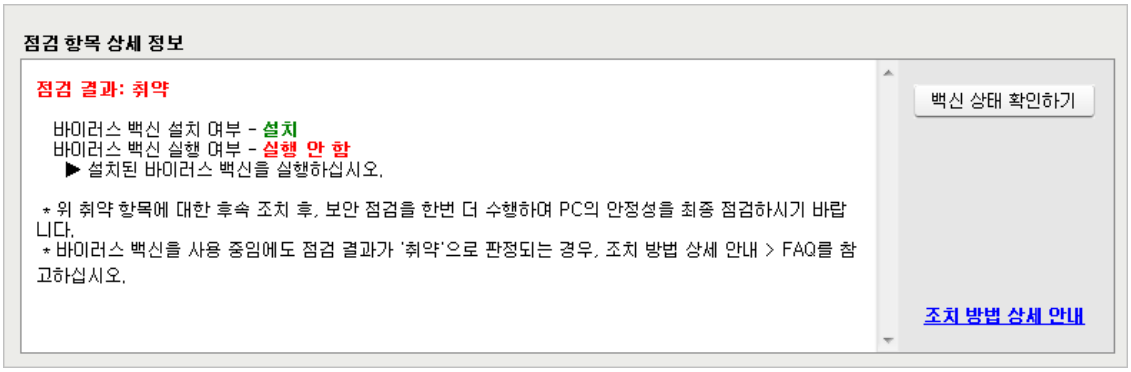
바이러스 백신 설치 및 실행 점검

바이러스 백신의 설치 및 실행 점검에 대한 조치 방법입니다. 바이러스 백신이 설치되지 않았거나, 실행 중이지 않은 경우는 다음과 같이 조치하여 주시기 바랍니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 의 바이러스 백신 설치 및 실행을 확인하였습니다.
- 취약: 점검 결과가 취약으로 나오는 경우, **바이러스 백신 설치 여부**와 **바이러스 백신 실행 여부**에 대한 상세 결과를 나타냅니다.
  - 바이러스 백신 설치 여부: **설치 안 함**으로 나타나면 백신 상태 확인하기를 눌러 관리 센터에 등록된 백신 정보가 있는지 확인합니다.
  - 바이러스 백신 실행 여부: **실행 안 함**으로 나타나면 백신 상태 확인하기를 눌러 Windows 관리 센터에서 바이러스 백신이 **사용 중**으로 표시되는지 확인합니다.



참고

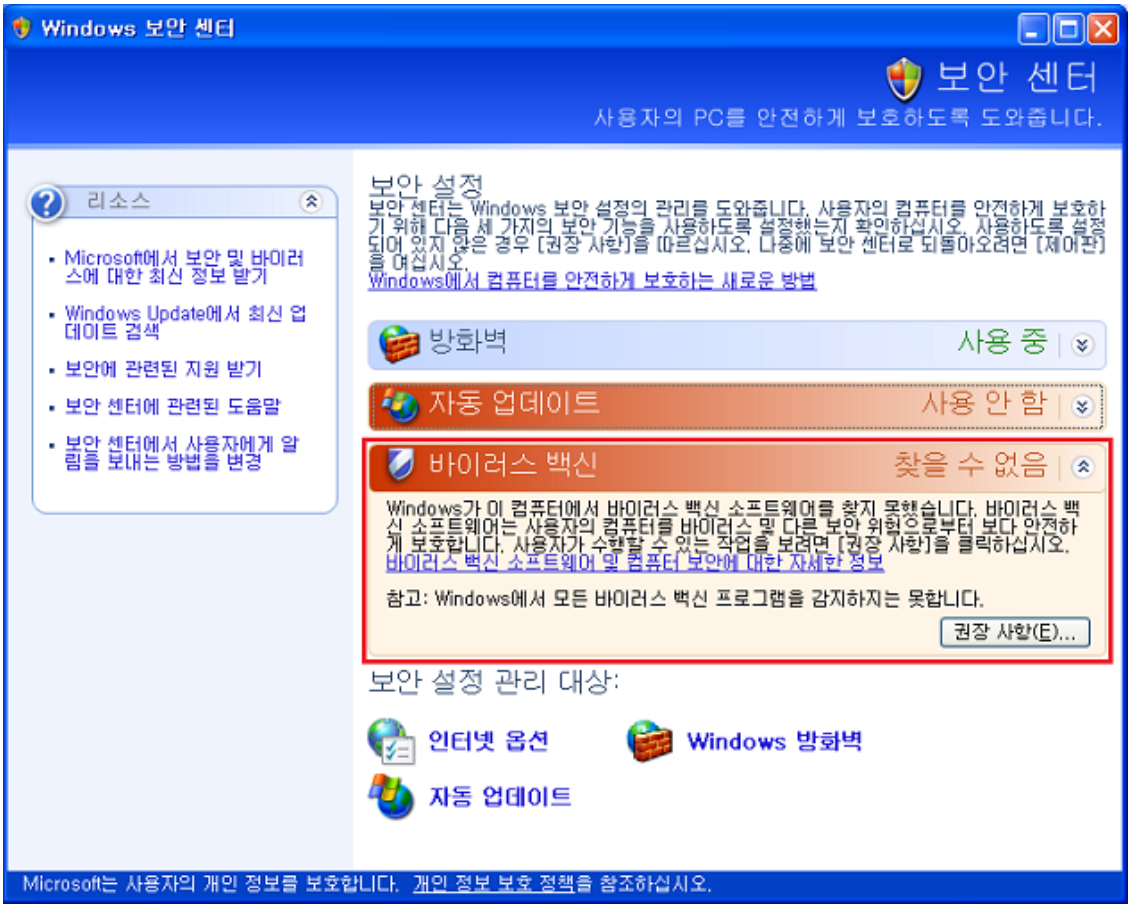
바이러스 백신이 설치/실행되고 있는데도 보안센터에 표시되지 않는 경우에는 FAQ 1. 바이러스 백신 설치 및 실행 점검을 참고하십시오. 바이러스 백신이 설치되어 있는데도 **찾을 수 없음**으로 표시되는 것은 바이러스 백신 정보를 Windows 의 보안센터에서 제공하지 않기 때문입니다.

조치 방법

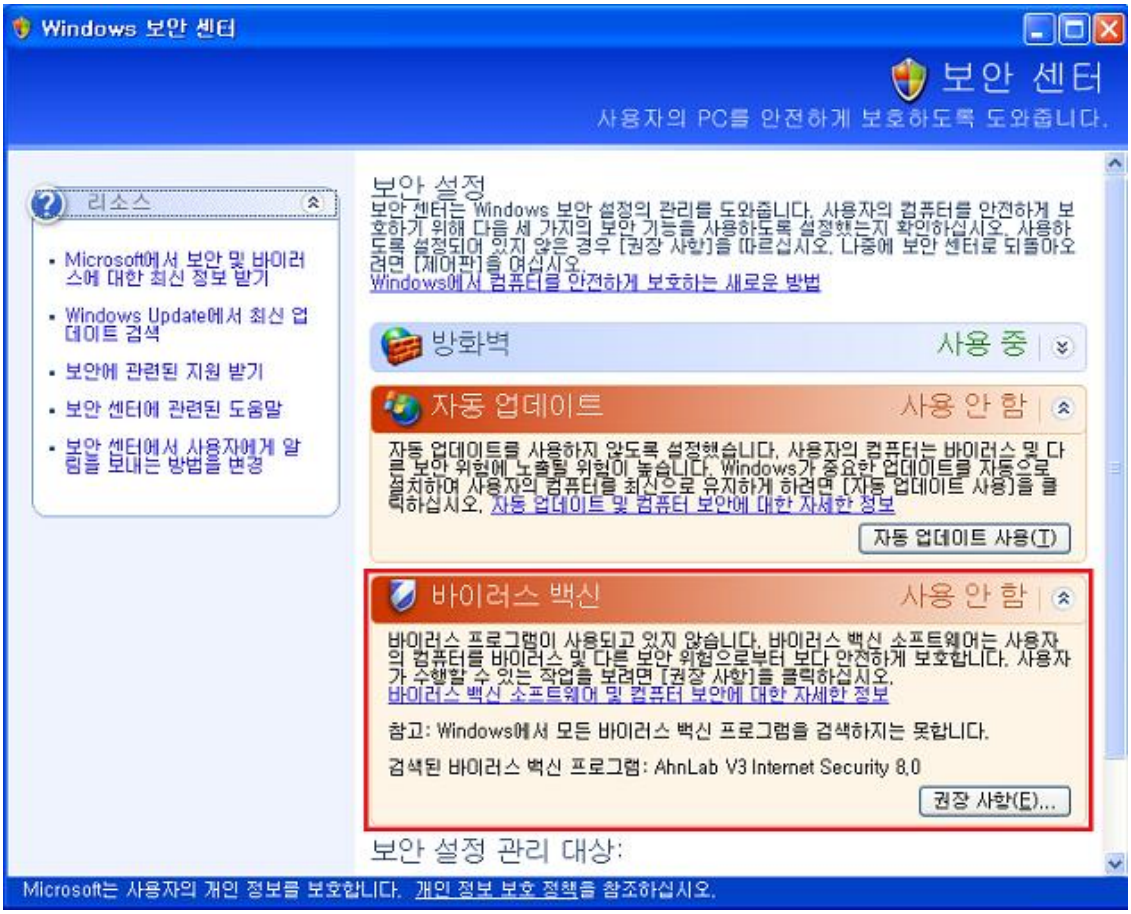
Windows XP, Windows Vista, Windows 7 시스템에서 바이러스 백신 설치 및 실행 여부를 확인하는 방법은 다음과 같습니다.

Windows XP SP2 이상

1. Windows 작업 표시줄의 **시작** > **설정** > **제어판**을 선택한 후 **클래식 보기로 전환**을 선택하여 **보안 센터**를 실행합니다.
2. 보안센터에서 바이러스 백신을 선택하여 설치된 바이러스 백신을 확인합니다.
   - 바이러스 백신이 설치되어 있지 않다면 **찾을 수 없음**으로 표시됩니다.



- 바이러스 백신이 설치되어 있으나 실행 중이지 않을 경우 **사용 안 함**으로 표시됩니다. 설치된 바이러스 백신을 실행하고 실시간 감시를 실행하십시오.

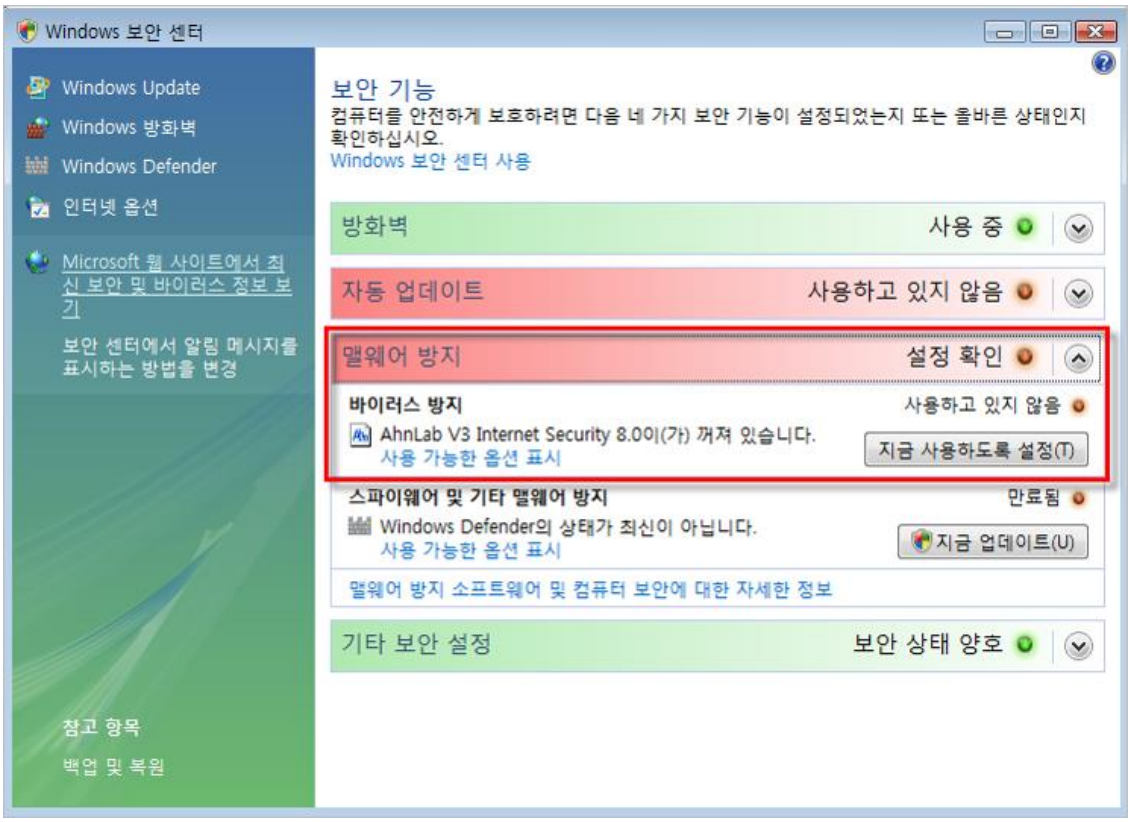


- 바이러스 백신이 설치되어 실행 중인 경우 점검 결과가 **안전**으로 표시되고 업데이트 상태에 따라 **최신 상태 아님, 사용** 중으로 표시됩니다.

Windows Vista

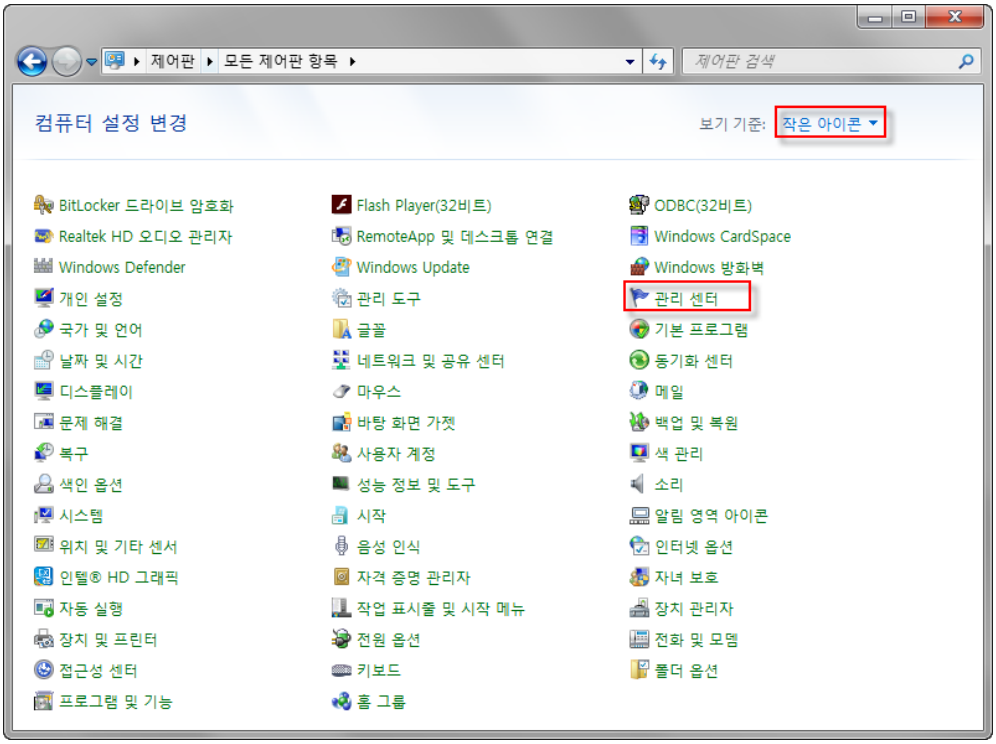
1. Windows 작업 표시줄의 **시작** > **설정** > **제어판**을 선택한 후 **클래식 보기로 전환**을 선택하여 **보안 센터**를 실행합니다.
2. 보안 센터에서 **맬 웨어 방지**를 선택하여 설치된 바이러스 백신을 확인합니다.
   - 바이러스 백신이 설치되어 있지 않다면 **찾을 수 없음**으로 표시됩니다.

- 바이러스 백신이 설치되어 있으나 실행 중이지 않을 경우 **사용하고 있지 않음**으로 표시됩니다. 설치된 바이러스 백신을 실행하고 실시간 감시를 실행합니다.



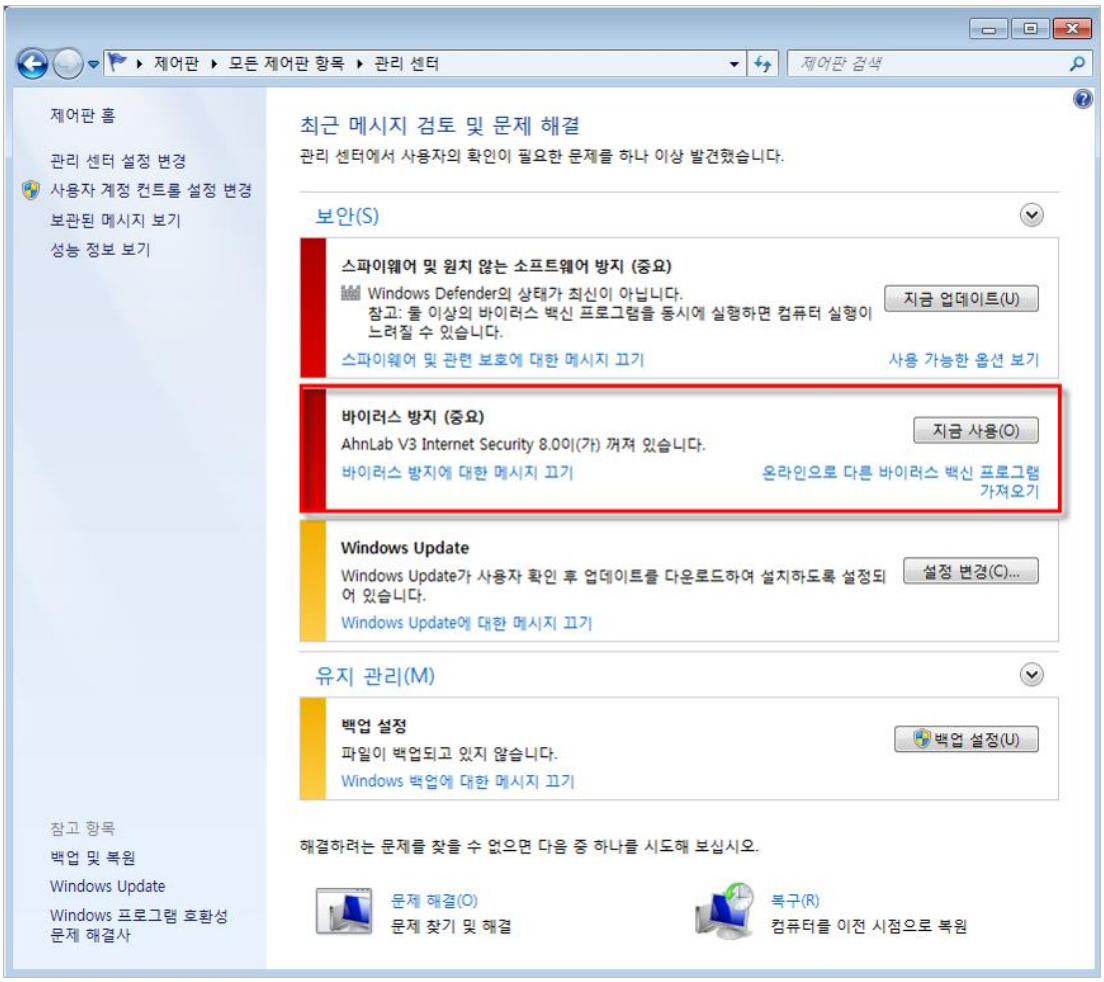
Windows 7

1. **시작** > **설정** > **제어판**에서 보기 기준을 작은 아이콘으로 전환하고 **관리 센터**를 선택합니다.



2. **보안**을 선택하고 **바이러스 방지**에 표시된 바이러스 백신 목록을 확인합니다.

- 바이러스 백신이 설치되지 않은 경우 **바이러스 백신 소프트웨어를 찾지 못했습니다.** 라고 표시됩니다.
- 바이러스 백신이 설치되어 있지 않다면 **찾을 수 없음**으로 표시됩니다.
- 바이러스 백신이 설치되어 있으나 실행 상태가 아니라면 **해당 백신이 꺼져 있습니다.** 라고 표시됩니다. **지금 사용**을 선택하여 바이러스 백신을 실행하고 실시간 검사를 실행합니다.



참고

바이러스 백신 설치 및 실행 점검은 Windows XP SP2 이상 시스템에서만 점검할 수 있습니다. 단, 설치된 백신 프로그램이 Windows 보안센터에 해당 프로그램에 대한 정보를 제공하지 않을 경우 내 PC 지키미 진단 결과와 다르게 나타날 수 있습니다.

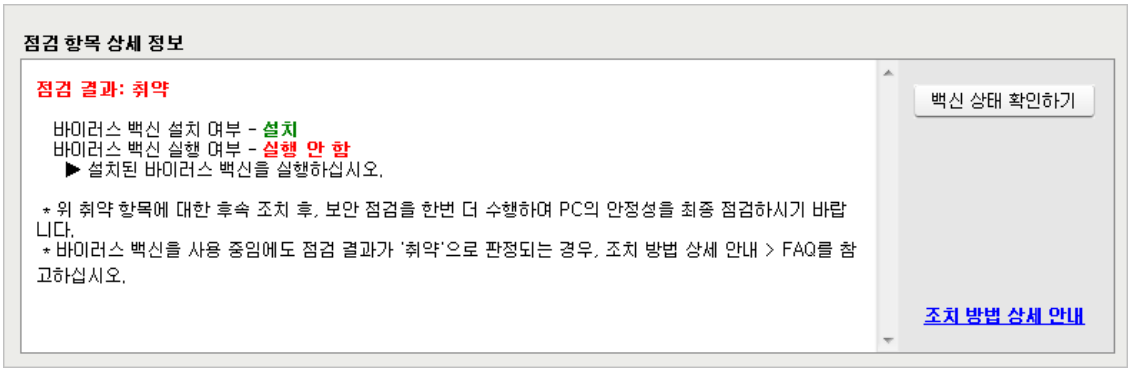
바이러스 백신의 최신 보안 패치 점검

바이러스 백신의 최신 보안 패치 점검에 대한 조치 방법입니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

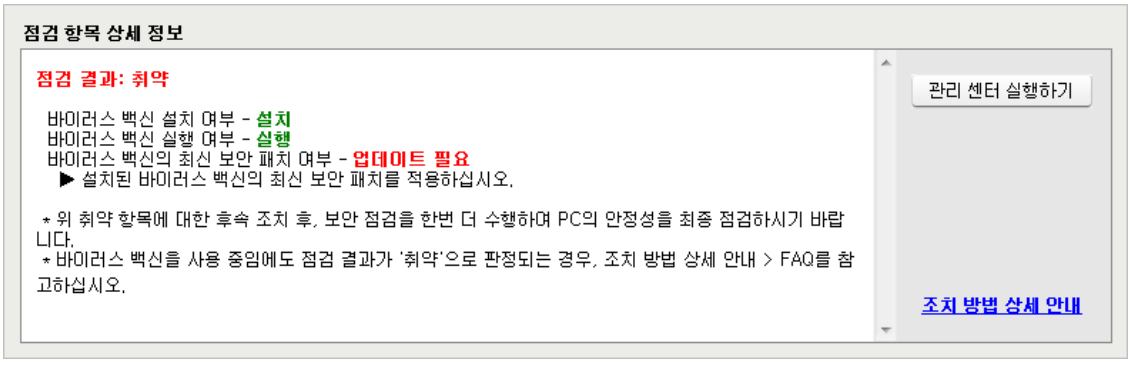
- 안전: PC 의 바이러스 백신이 최신으로 유지되고 있음을 확인하였습니다.
- 취약: 점검 결과가 취약으로 나오는 경우, **바이러스 백신 설치 여부**와 **바이러스 백신 실행 여부**에 대한 상세 결과를 나타냅니다.
- 바이러스 백신 설치 여부: **설치 안 함**으로 나타나면 백신 상태 확인하기를 눌러 관리 센터에 등록된 백신 정보가 있는지 확인합니다.
- 바이러스 백신 실행 여부: **실행 안 함**으로 나타나면 백신 상태 확인하기를 눌러 Windows 관리 센터에서 바이러스 백신이 **사용 중**으로 표시되는지 확인합니다.



참고

바이러스 백신이 설치/실행되고 있는데도 보안 센터에 표시되지 않는 경우에는 FAQ 1. 바이러스 백신 설치 및 실행 점검을 참고하십시오.

- 바이러스 백신의 최신 보안 패치 여부: **업데이트 필요**로 나타나면 **관리 센터 실행하기**를 눌러 보안 센터에 등록된 바이러스 백신이 최신 업데이트 상태인지 확인합니다.



참고

바이러스 백신이 최신 업데이트 상태인 경우에도 점검 결과가 **취약**으로 표시될 경우에는 FAQ 2. 바이러스 백신 최신 패치 점검을 참고하십시오.

조치 방법

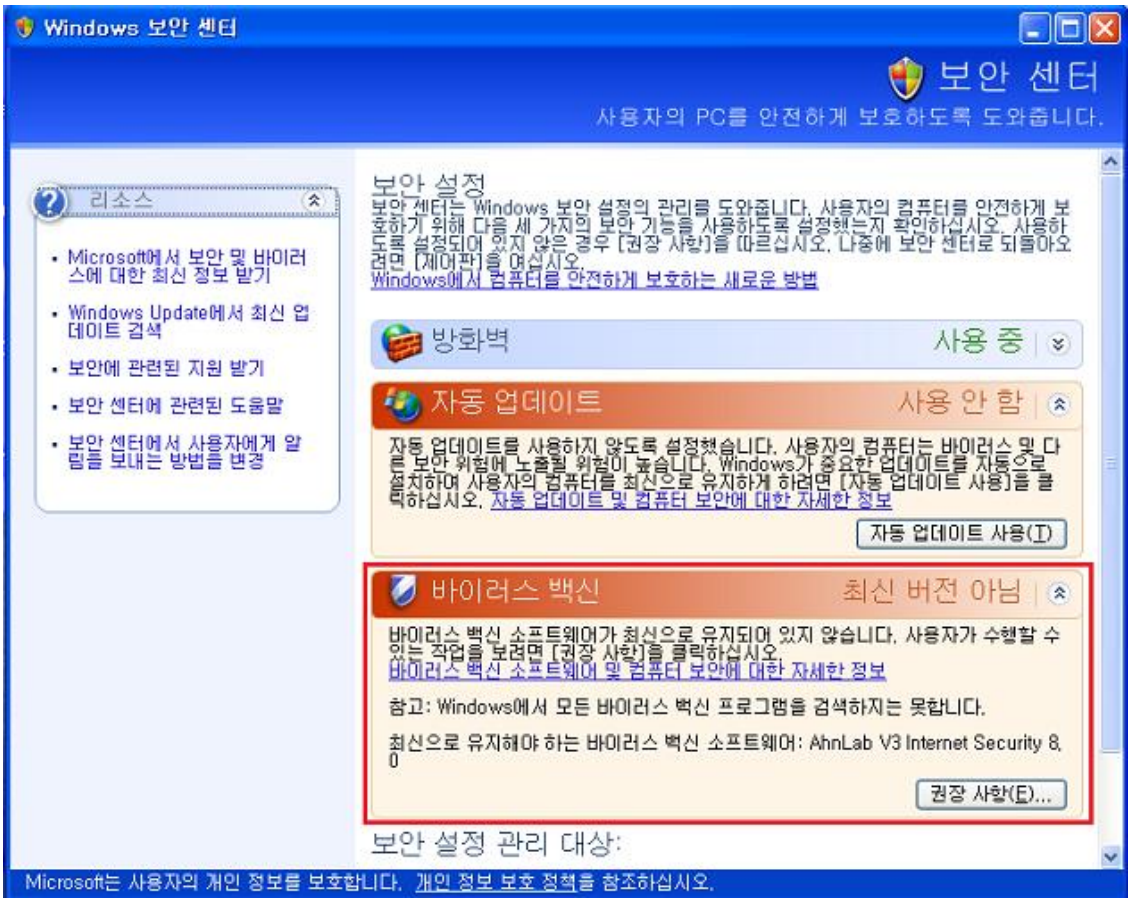
바이러스 백신 최신 업데이트 상태를 확인하는 방법은 다음과 같습니다.

Windows XP SP2 이상 버전

1. Windows 작업 표시줄의 **시작** > **설정** >**제어판**을 선택한 후 **클래식 보기로 전환**을 선택하여 **보안 센터**를 실행합니다.
2. 보안 센터에서 바이러스 백신을 선택하여 설치된 바이러스 백신을 확인합니다.
   - 바이러스 백신이 최신 엔진으로 업데이트된 상태가 아니라면 **최신 버전 아님**으로 표시됩니다. 설치된 바이러스 백신의 업데이트를 실행합니다.
   - 바이러스 백신이 최신 엔진으로 업데이트된 상태라면 **사용 중**으로 표시됩니다.

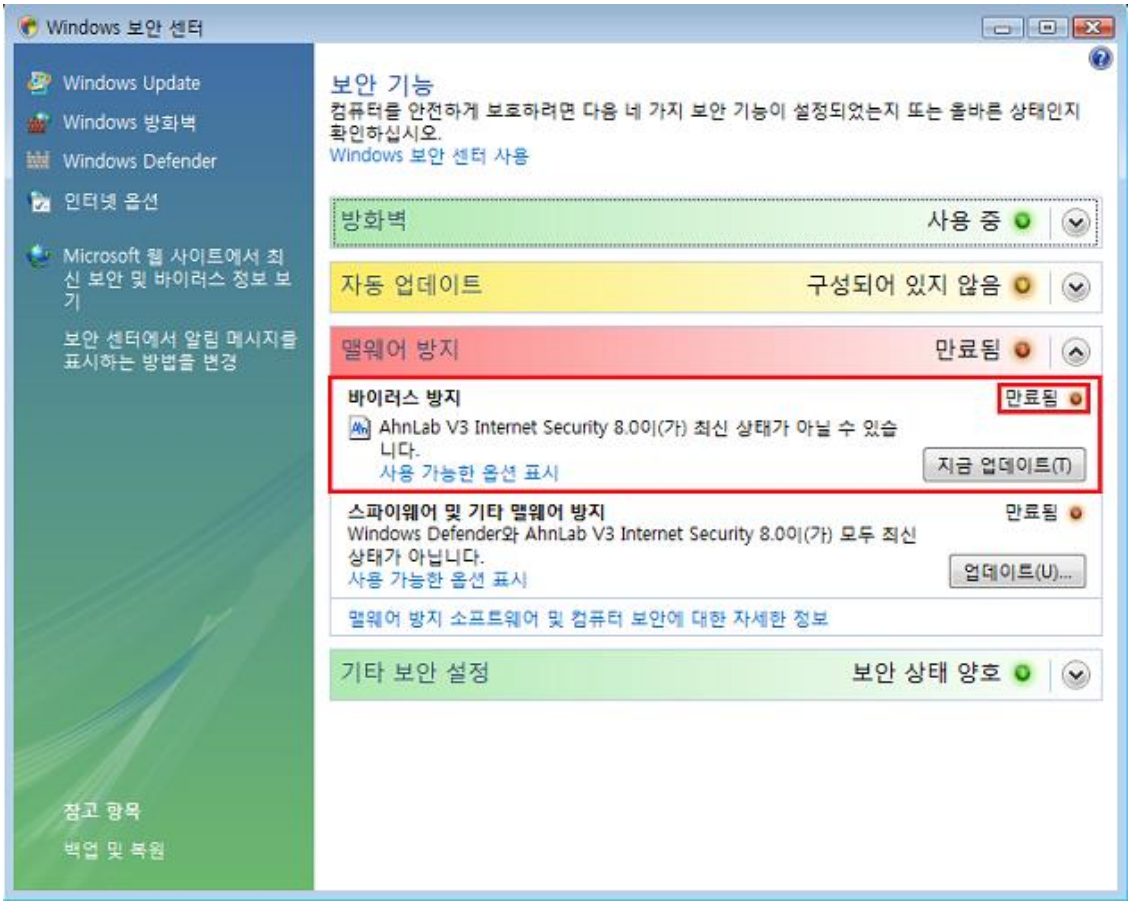
참고

바이러스 백신이 최신 업데이트 상태인데도 **최신 버전 아님**으로 표시되는 것은 바이러스 백신이 업데이트 정보를 Windows 의 보안 센터에서 제공하지 않기 때문입니다.



Windows Vista

1. Windows 작업 표시줄의 **시작** > **설정** > **제어판**을 선택한 후 **클래식 보기로 전환**을 선택하여 **보안 센터**를 실행합니다.
2. 보안 센터에서 **맬 웨어 방지**를 선택하여 설치된 바이러스 백신을 확인합니다.
   - 바이러스 백신이 최신 업데이트 상태가 아니라면 만료됨으로 표시됩니다. 설치된 바이러스 백신의 업데이트를 실행합니다.

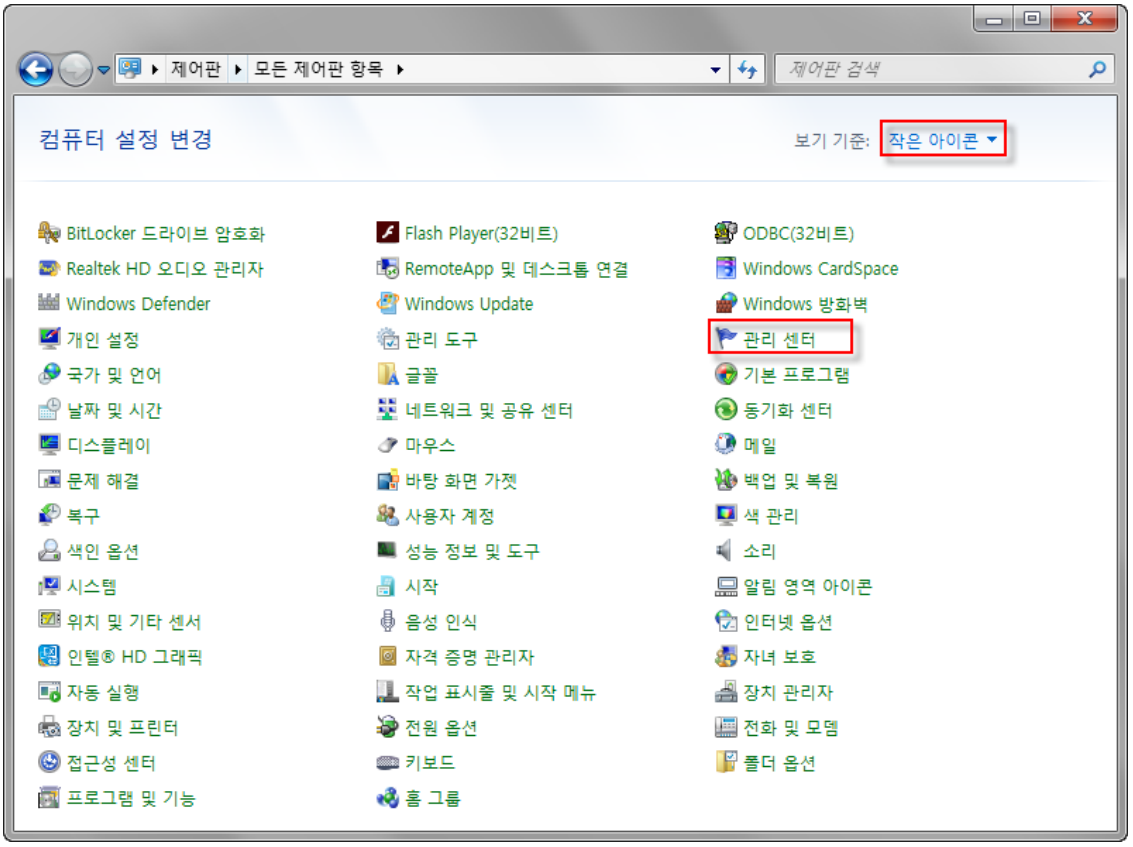


참고

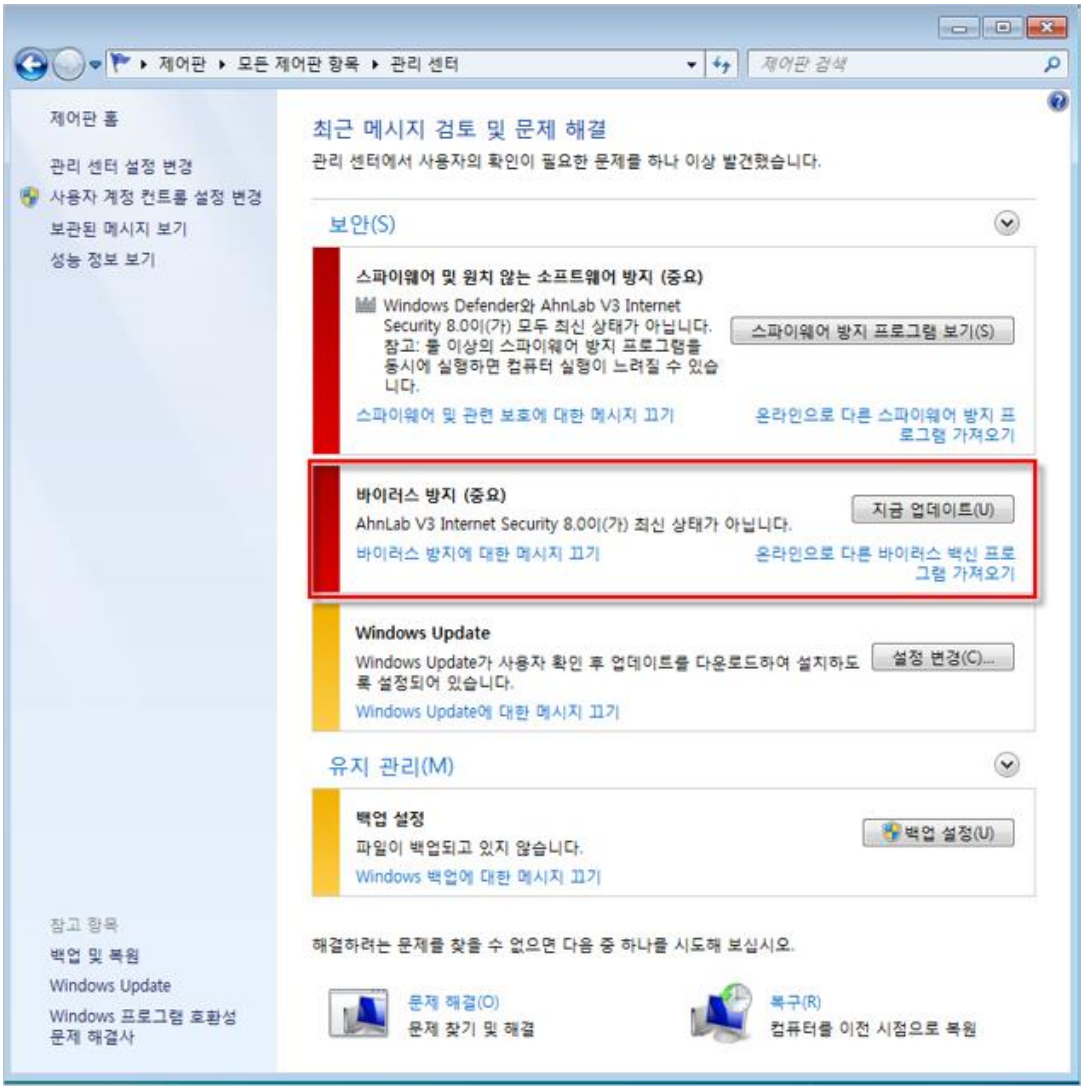
바이러스 백신이 최신 업데이트 상태인데도 **최신 버전 아님**으로 표시되는 것은 운영 체제에 맞는 내 PC 지키미를 설치하지 않았거나 바이러스 백신이 업데이트 정보를 Windows 의 보안 센터에서 제공하지 않기 때문입니다.

Windows 7

1. **시작** > **설정** > **제어판**에서 보기 기준을 작은 아이콘으로 전환하고 **관리 센터**를 선택합니다.



2. **보안**을 선택하고 **바이러스 방지**에 표시된 바이러스 백신 목록을 확인합니다.
   - 바이러스 백신이 최신 업데이트 상태가 아닌 경우 **최신 상태가 아닙니다.** 라고 표시됩니다. **지금 업데이트**를 눌러 바이러스 백신의 업데이트를 실행합니다.



참고

바이러스 백신이 최신 업데이트 상태인데도 **최신 상태가 아닙니다.** 로 표시되는 것은 바이러스 백신의 정보를 Windows 의 보안 센터에서 제공하지 않기 때문입니다.

- 바이러스 백신 제품 업데이트 사이트 안내

바이러스 백신 제작사의 홈페이지에서 업데이트 방법을 확인하고 최신 엔진 버전을 유지하시기 바랍니다.

  - 안랩 V3 다운로드 사이트 바로가기

참고

바이러스 백신의 최신 보안 패치 점검은 Windows XP SP2 이상 시스템에서만 점검할 수 있습니다. 단, 설치된 백신 프로그램이 Windows 보안 센터에 해당 프로그램에 대한 정보를 제공하지 않을 경우 내 PC 지키미 진단 결과와 다르게 나타날 수 있습니다.

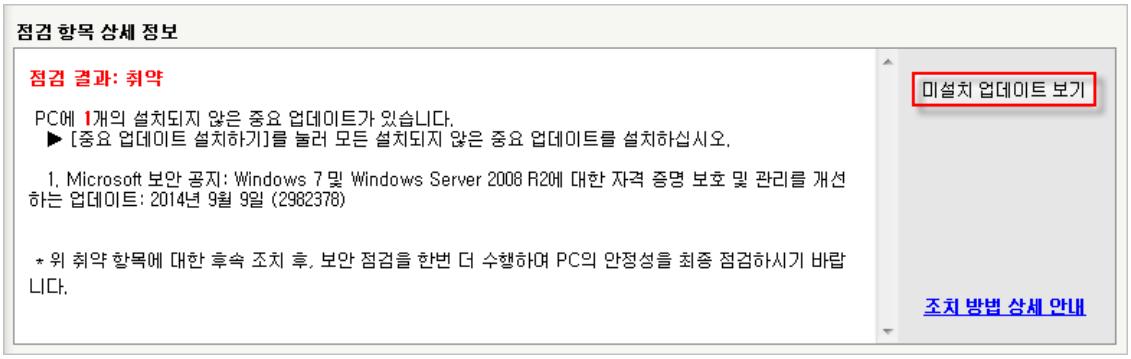
운영 체제, MS Office 최신 보안 패치 점검

Windows 운영 체제 및 MS Office 의 보안 패치 상태를 점검하여 최신 보안 업데이트 적용 여부를 점검합니다. 점검 결과가 **안전**인 상태는 MS 에서 중요 업데이트로 지정한 업데이트 항목을 모두 설치한 상태를 의미합니다. 점검 결과가 안전에서 취약으로 변경되는 경우는 MS 에서 중요 업데이트가 새롭게 공지된 것이므로 Windows Update 를 실행하거나 최신 보안 패치 파일을 다운로드 하여 설치하시기 바랍니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 의 운영 체제 및 MS Office 가 최신 상태입니다. Microsoft 에서 지정한 중요 업데이트가 모두 설치되어 있는 경우에만 점검 결과가 **안전**으로 표시됩니다.
- 취약: 점검 결과가 취약으로 나오는 경우, PC 에 설치되지 않는 중요 업데이트가 존재하는 것으로 나옵니다. **미설치 업데이트 보기**를 눌러 설치되지 않은 중요 업데이트를 설치하십시오.

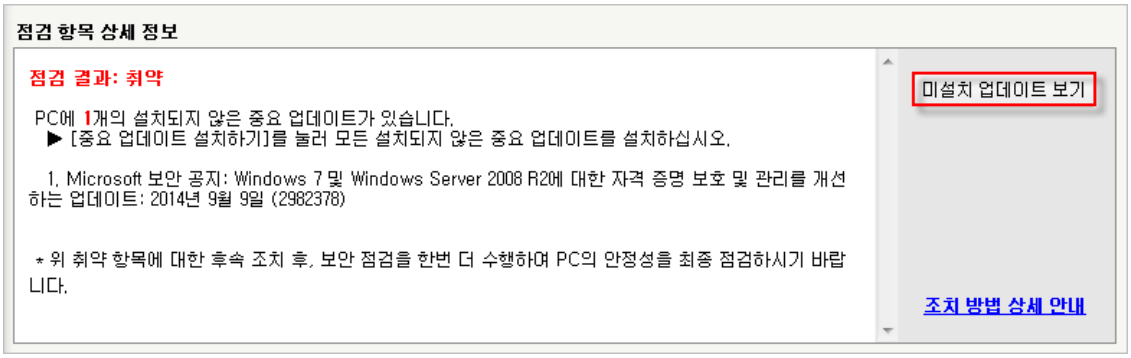


조치 방법

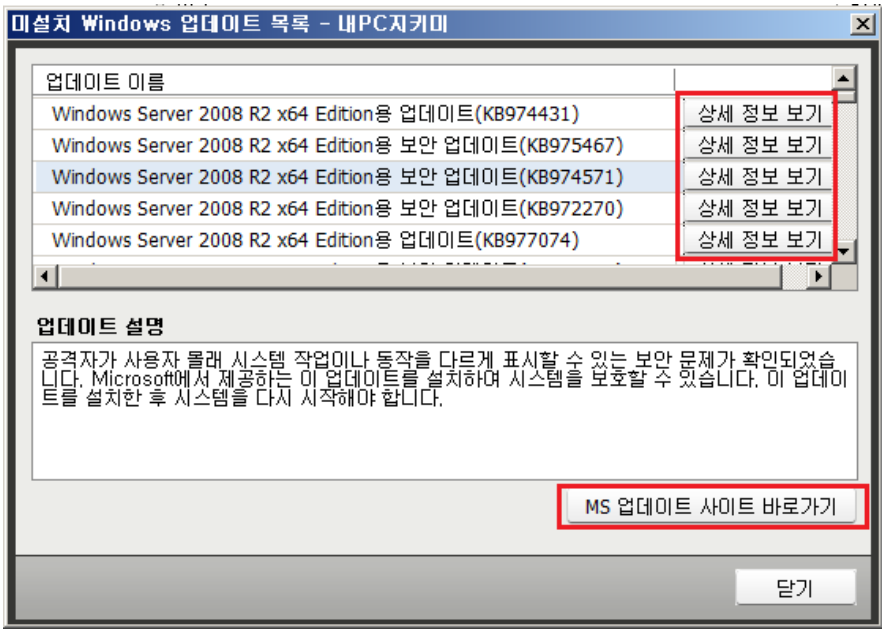
점검 결과가 **취약**일 때, APM 라이선스가 없는 경우와 APM 라이선스가 있는 경우에 따라 다음과 같이 조치하여 주시기 바랍니다.

[APM 라이선스가 없는 경우]

1. 미설치 업데이트 보기를 누릅니다.



2. <미설치 Windows 업데이트 목록>이 표시됩니다.



참고

MS 업데이트 서버와의 연결이 원활하지 않은 경우 해당 항목이 점검 목록에 표시되지 않습니다.

- 업데이트 이름: 업데이트 이름 목록에서 항목을 선택하면 아래 쪽에 선택한 업데이트에 대한 설명이 표시됩니다.
- 상세 정보 보기: 업데이트에 대한 정보와 사이트 정보를 표시합니다.
- MS 업데이트 사이트 바로 가기: MS 업데이트 사이트로 연결합니다. MS 업데이트 사이트에 접속하면 사용자 PC 에 설치된 MS 제품 군에 대한 업데이트를 실행할 수 있습니다.

참고

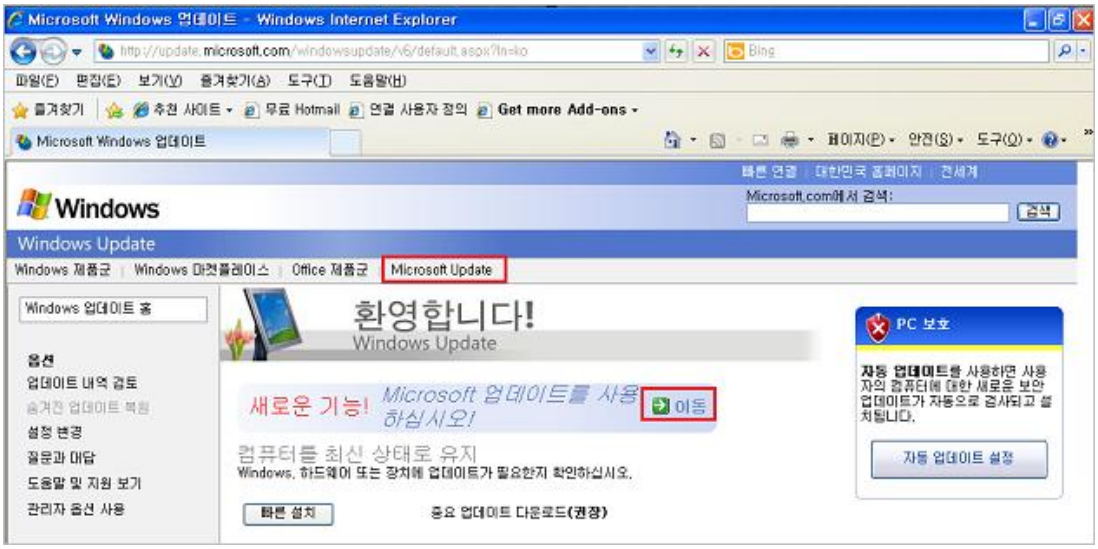
정식 라이선스로 설치하지 않은 불법 복제된 MS 제품의 경우, MS 업데이트가 실행되지 않습니다.

Windows XP

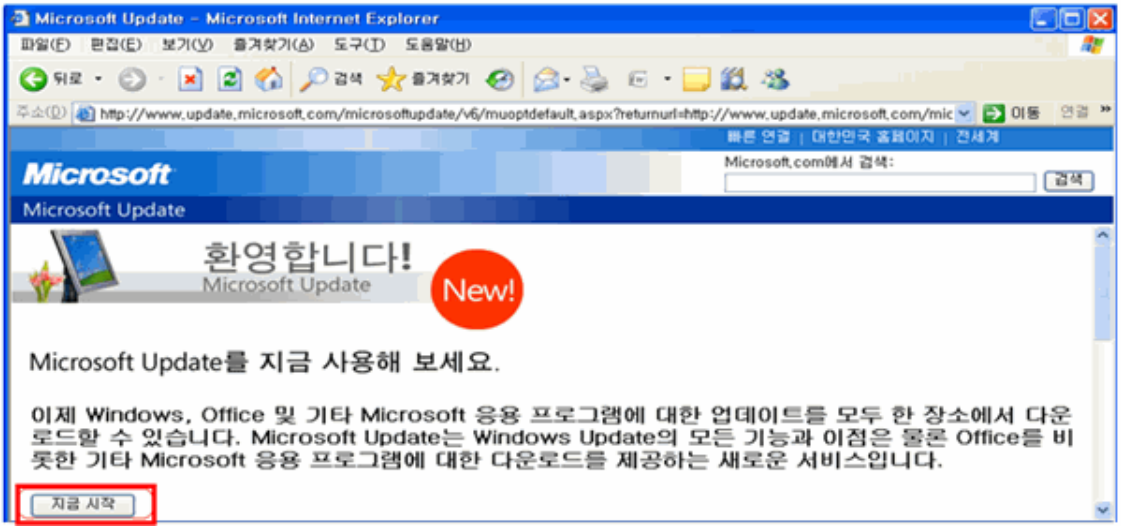
1. IE 실행 후 **도구** > **Windows Update**를 선택하거나 http://www.update.microsoft.com로 접속합니다.
2. **Microsoft Update**를 선택하거나 **새로운 기능!** 옆에 있는 **이동**을 누르십시오.

참고

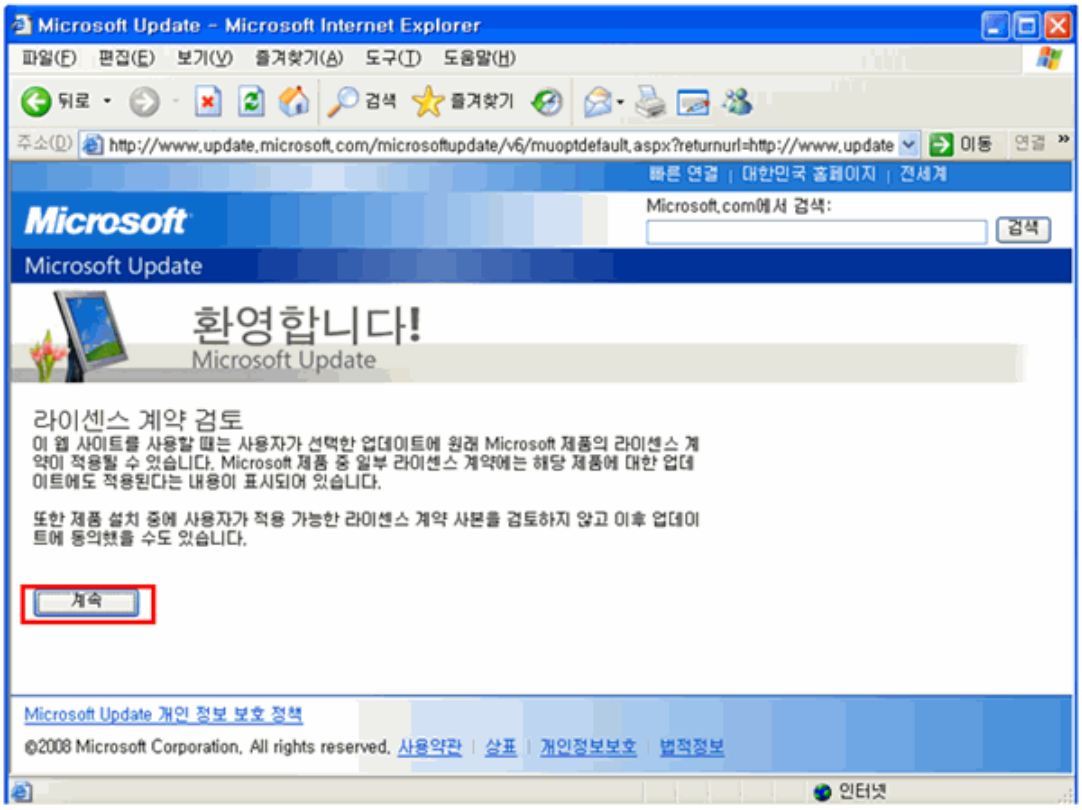
이전에 Windows 및 MS office 제품에 대한 업데이트를 적용한 적이 있는 경우에는 아래 사용자 지정 설치로 이동하십시오.



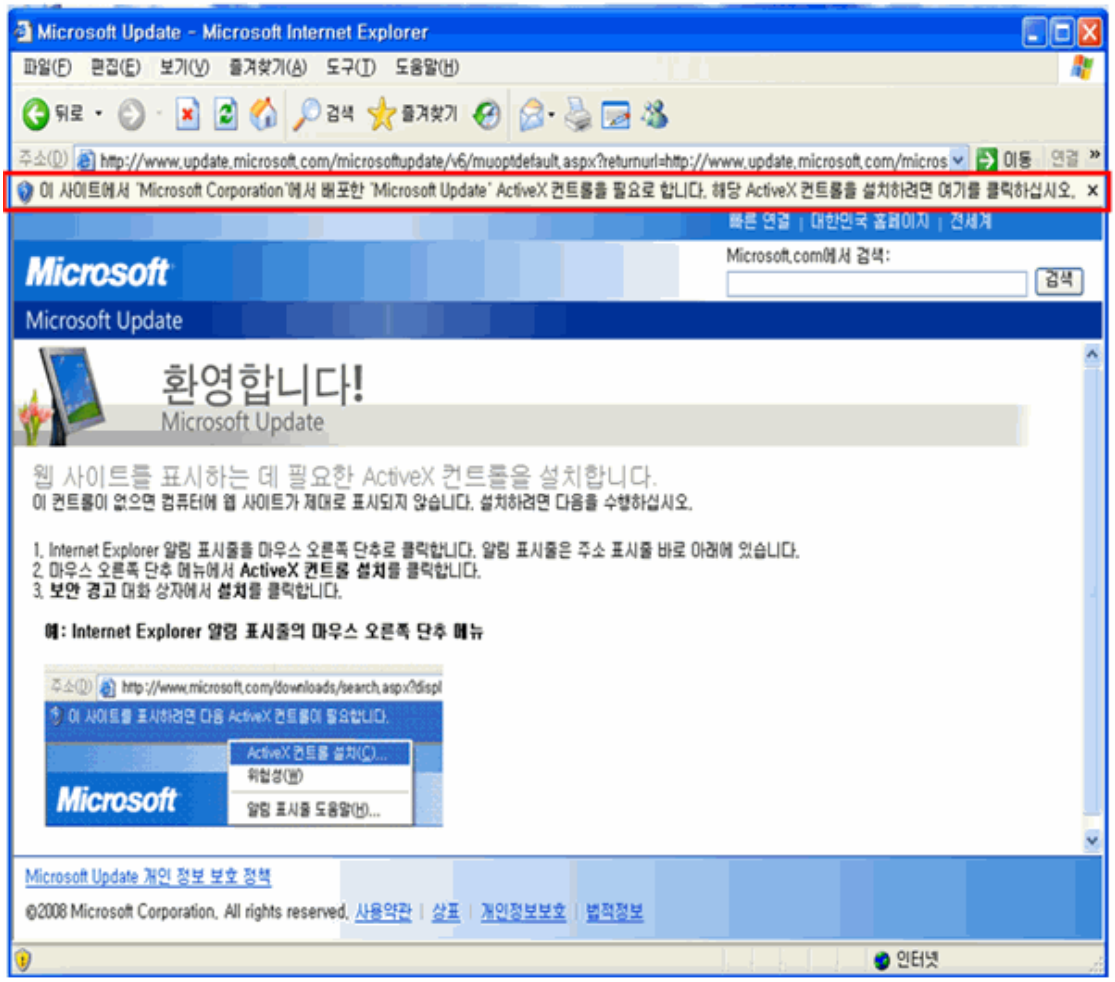
3. 환영합니다. 화면이 표시되면 **지금 시작**을 눌러 Microsoft Update를 진행합니다.



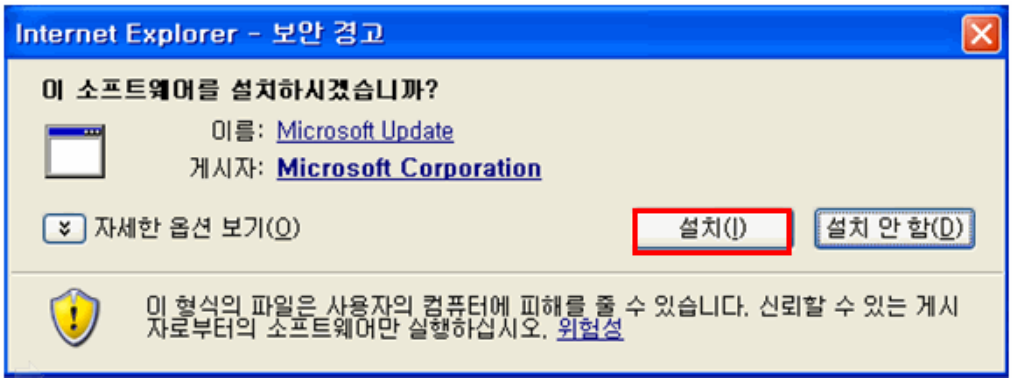
4. **계속**을 누릅니다.



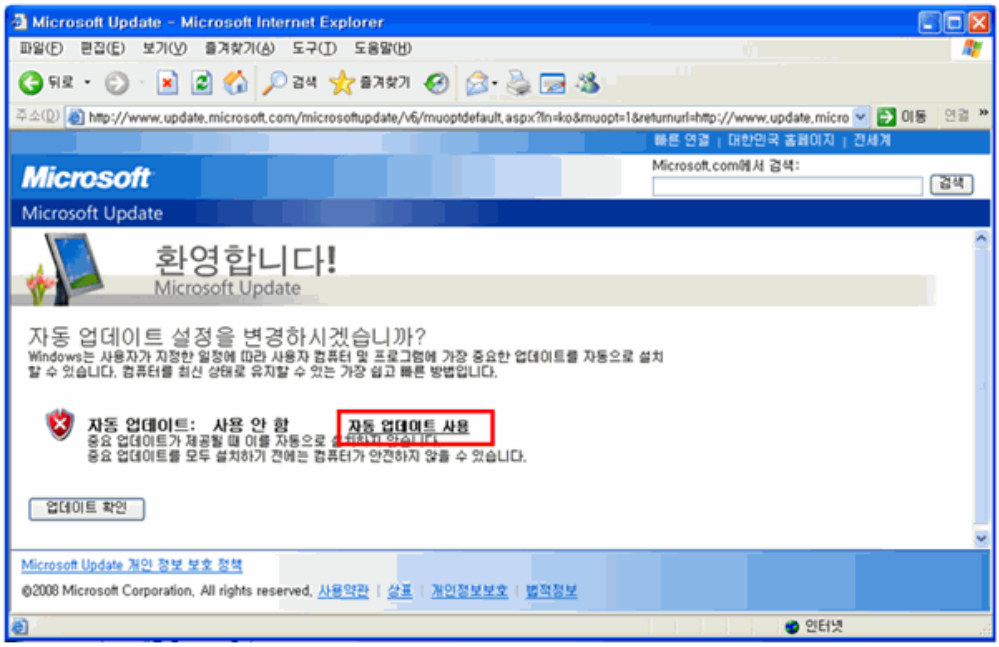
5. IE 알림 표시줄에서 마우스 오른쪽을 눌러 **ActiveX 컨트롤 설치**를 누릅니다.



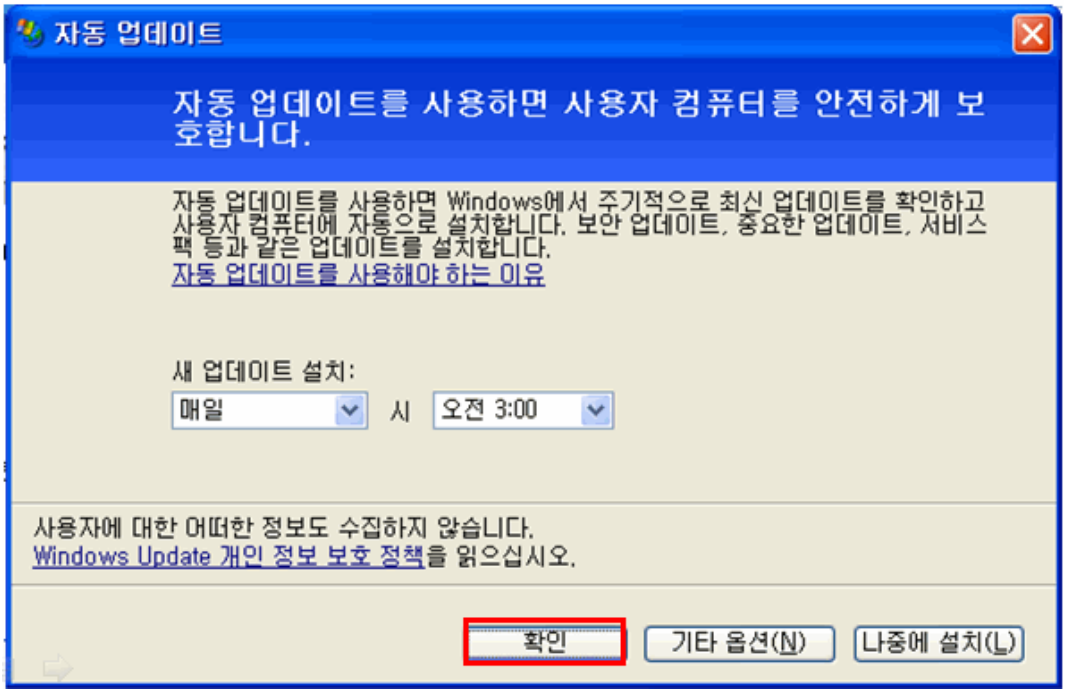
6. <보안 경고>가 나타나면 설치할 소프트웨어 이름을 확인하고 **설치**를 누릅니다.



7. 자동 업데이트 설정이 되어 있지 않은 경우 아래 화면과 같이 자동 업데이트 사용 설정 화면이 나타납니다. **자동 업데이트 사용**을 누릅니다.



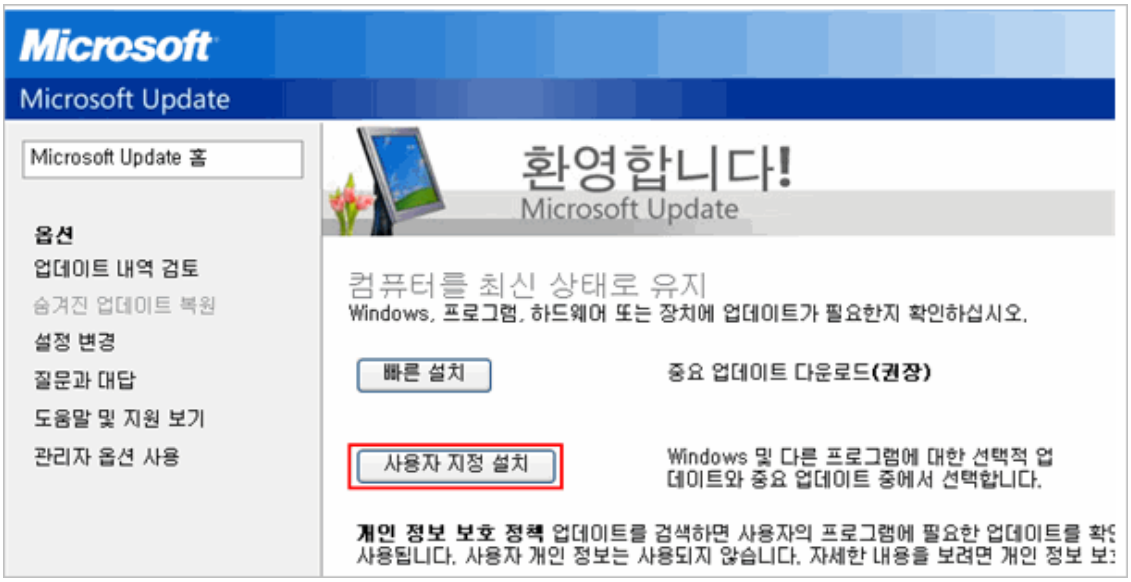
8. <자동 업데이트>가 나타나면 새 업데이트 설치에서 **매일**로 설정합니다. 매일로 시간을 설정하면 설정된 시간에 자동 업데이트가 수행됩니다.



사용자 지정 설치

사용자 지정 설치를 선택하면 업데이트 항목을 사용자가 확인하고 설치할 수 있습니다.

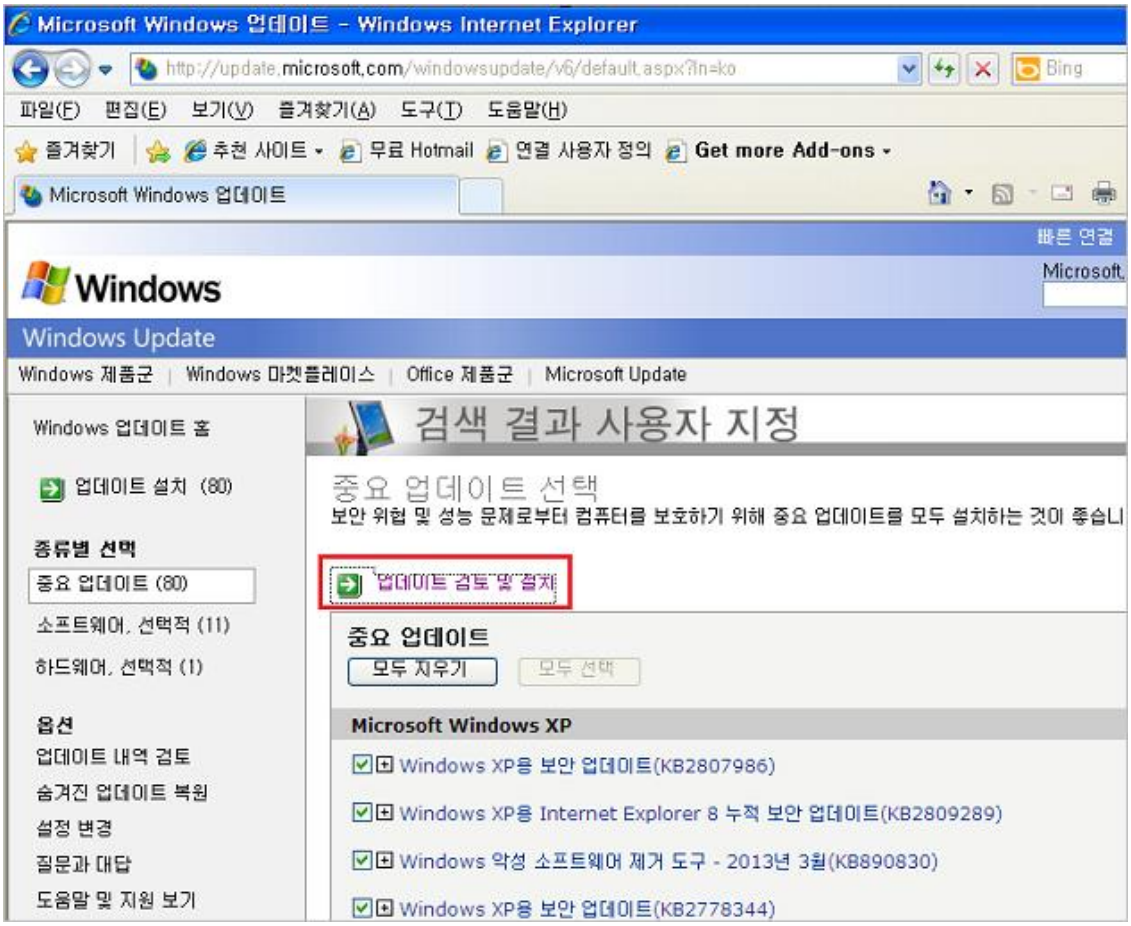
1. IE 실행 후 **도구** > **Windows Update**를 선택하거나 http://www.update.microsoft.com로 접속한 후 **사용자 지정 설치**를 누릅니다.



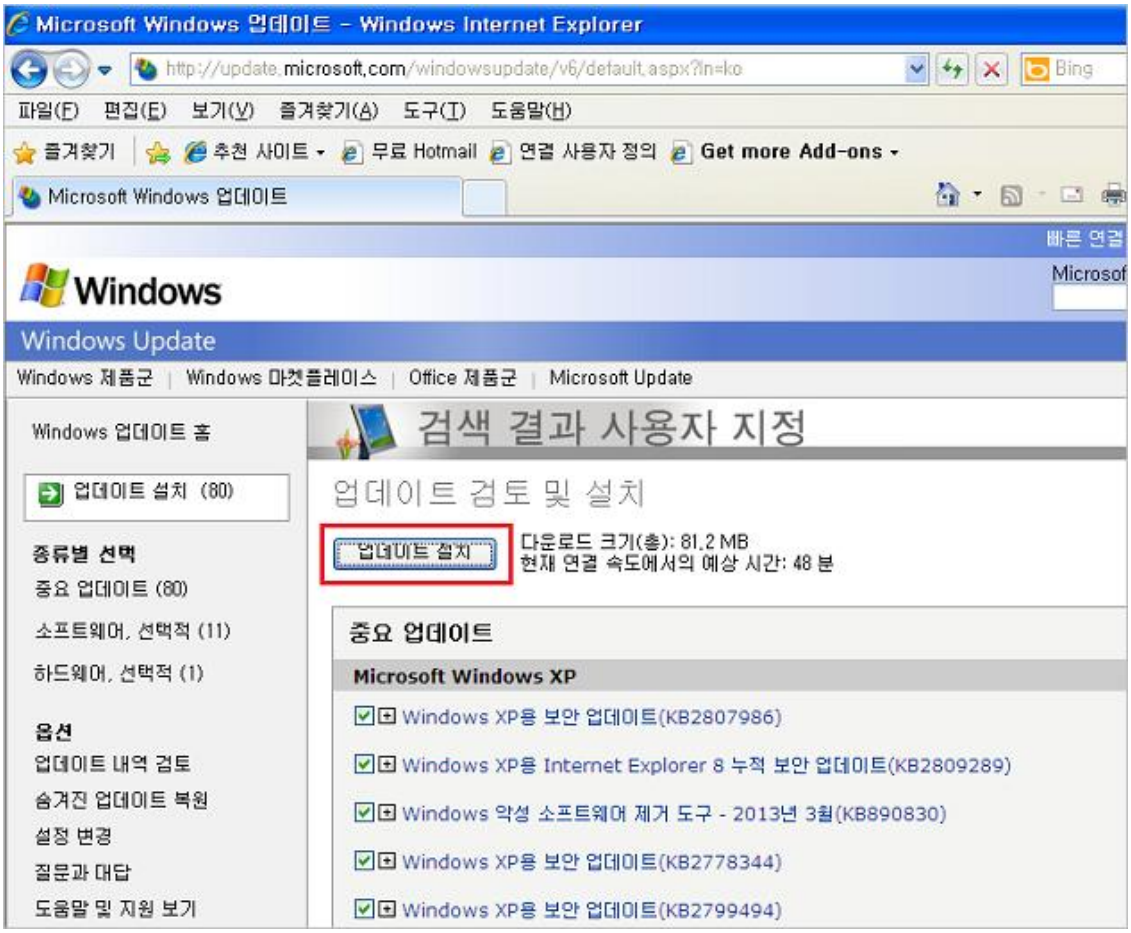
2. 업데이트 목록이 나타나면 **업데이트 검토 및 설**치를 눌러 설치를 시작합니다.

참고

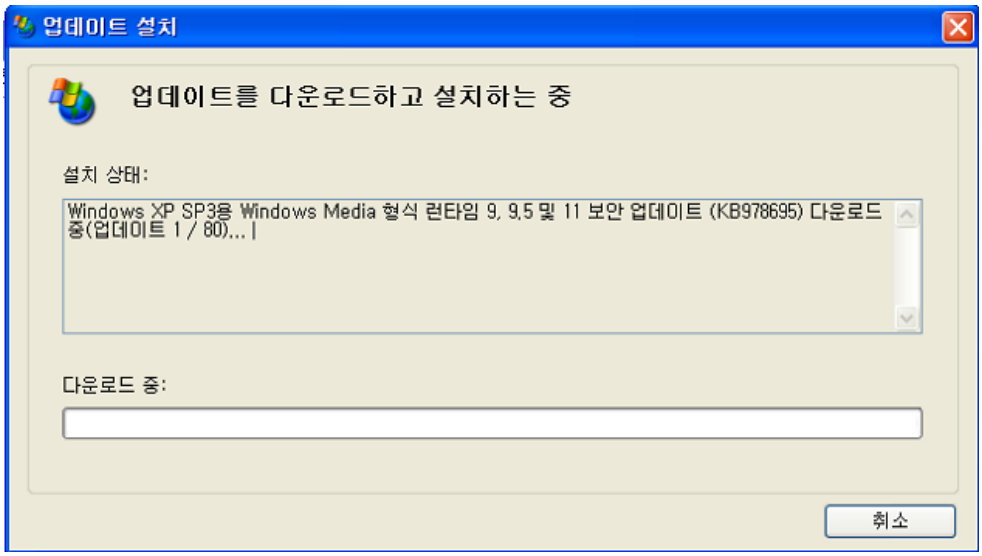
해당 업데이트에 대한 자세한 정보를 확인하려면 해당 업데이트를 누르면 정보가 표시됩니다. 설치하지 않을 항목에 대해서는 업데이트 숨기기를 설정하면 점검 대상에서 제외됩니다.



3. **업데이트 설치**를 누릅니다.



4. <업데이트 설치>에서 업데이트 파일을 다운로드 한 후 설치합니다.



참고

업데이트를 모두 마친 후 Windows Update 사이트에 다시 접속하여 누락된 중요 업데이트가 있는지 확인할 수 있습니다.

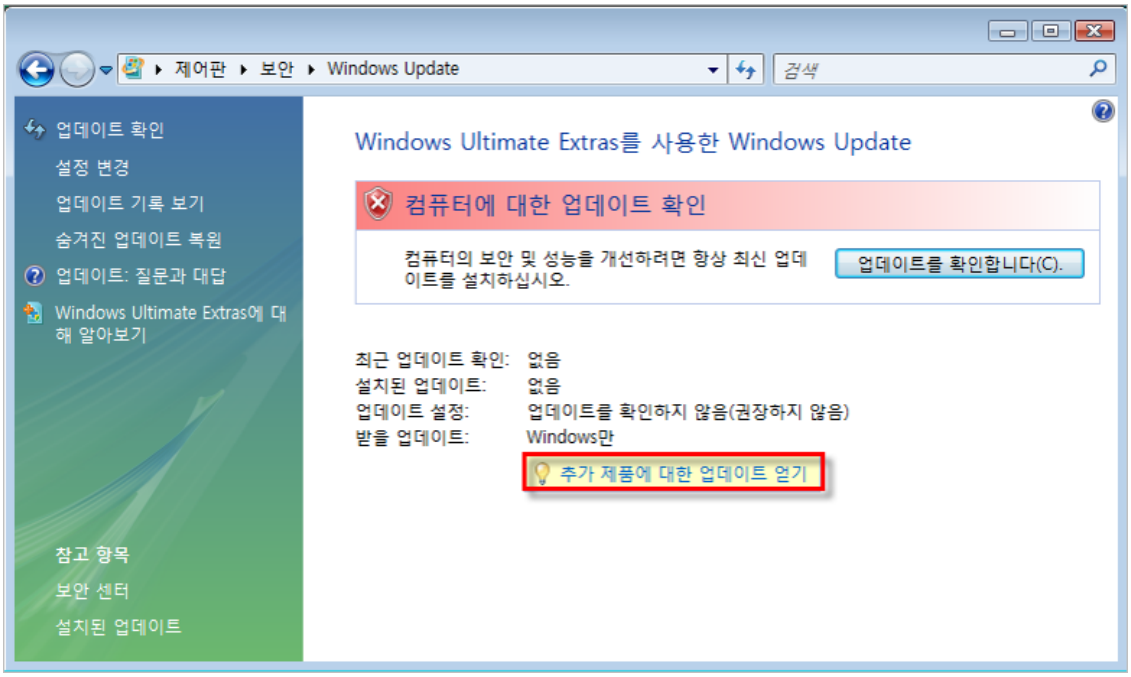
Windows Vista

1. 작업 표시줄의 **시작** > **모든 프로그램**에서 **Windows Update**를 선택합니다.

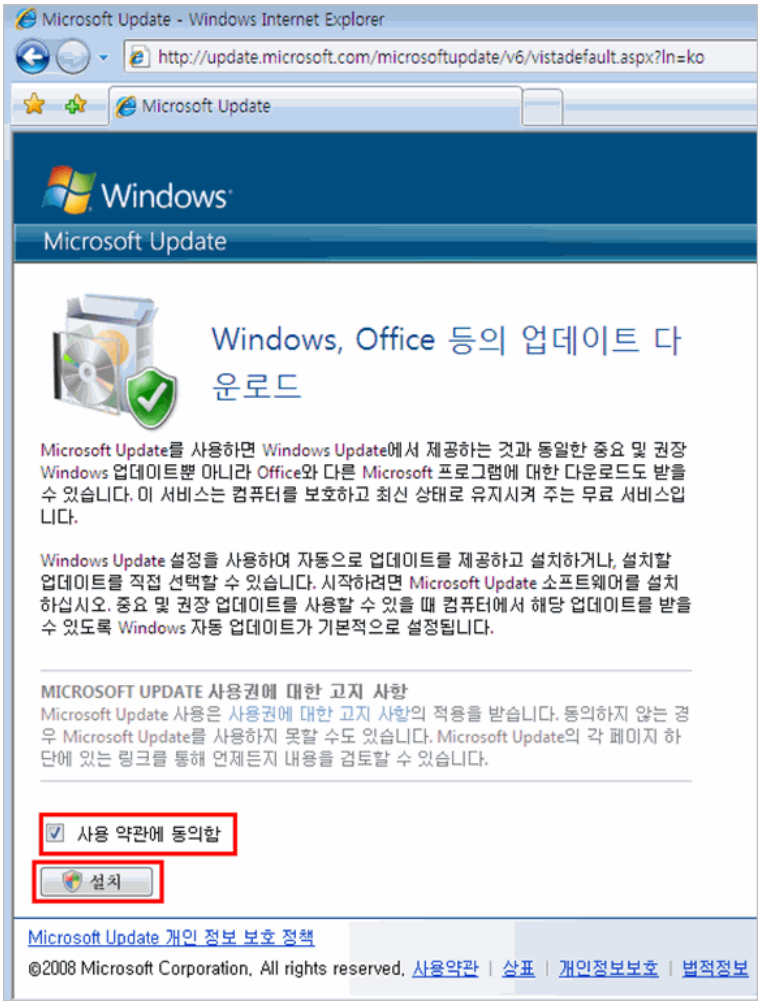
참고

이전에 Windows 및 MS office 제품에 대한 업데이트를 적용한 적이 있는 경우에는 아래 업데이트 설치로 이동하십시오.

2. Windows와 MS Office에 대한 최신 업데이트를 설치하려면 **추가 제품에 대한 업데이트 얻기**를 선택합니다.



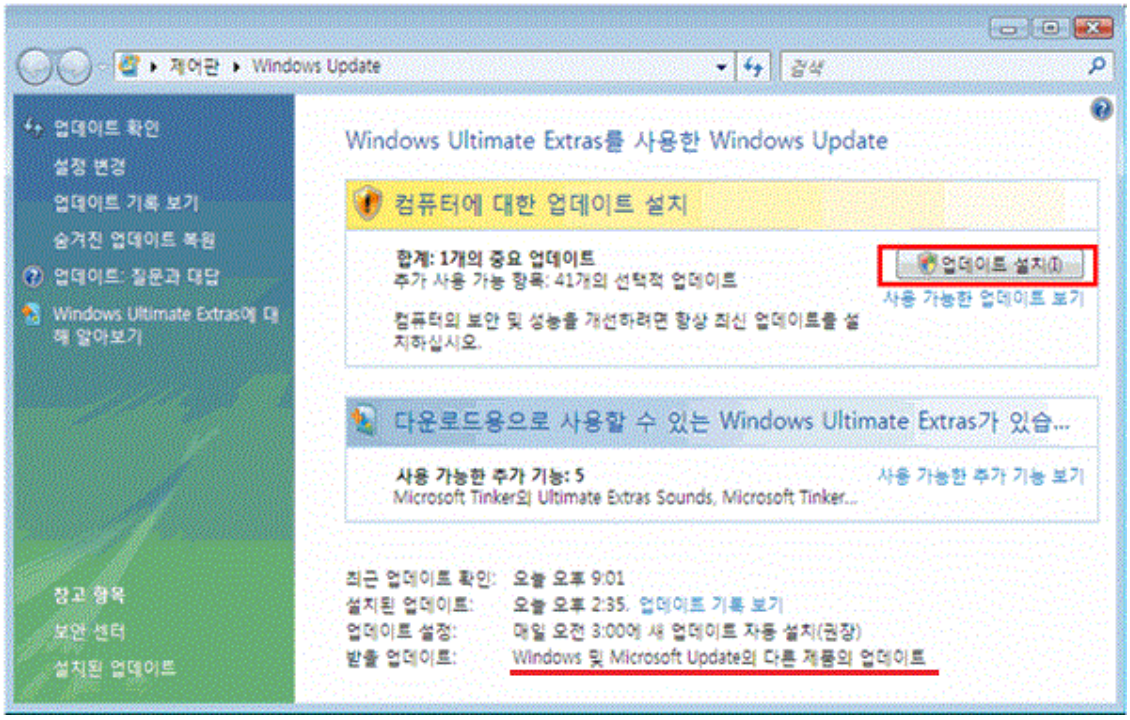
3. IE가 실행되면 **사용 약관에 동의함**을 선택하고 **설치**를 눌러 Microsoft Update를 사용하도록 설정합니다.



4. Microsoft Update를 마치면 다음 화면과 같이 설치 완료 알림 화면이 나타납니다.

업데이트 설치

1. 작업 표시줄의 **시작** > **모든 프로그램**에서 **Windows Update**를 선택합니다.
2. 제어판의 Windows Update가 나타나면 **업데이트 설치**를 누릅니다.

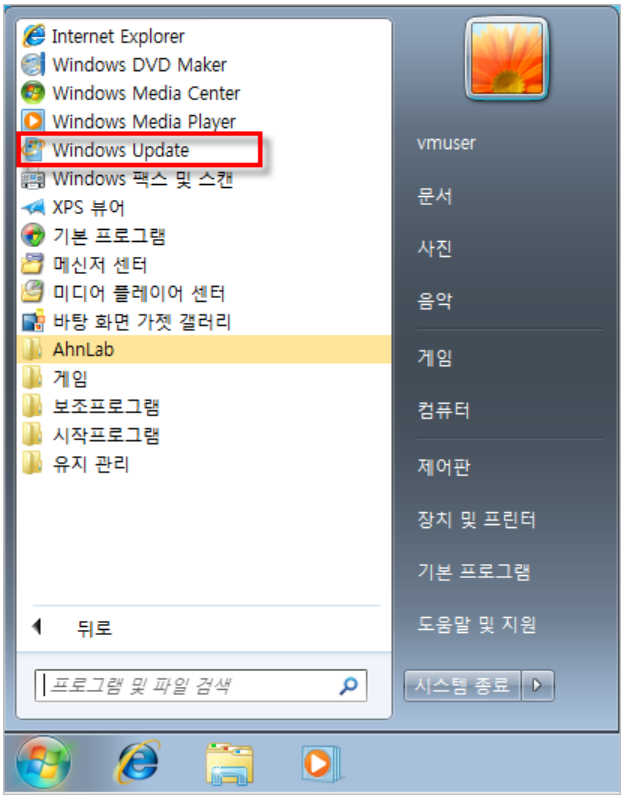


참고

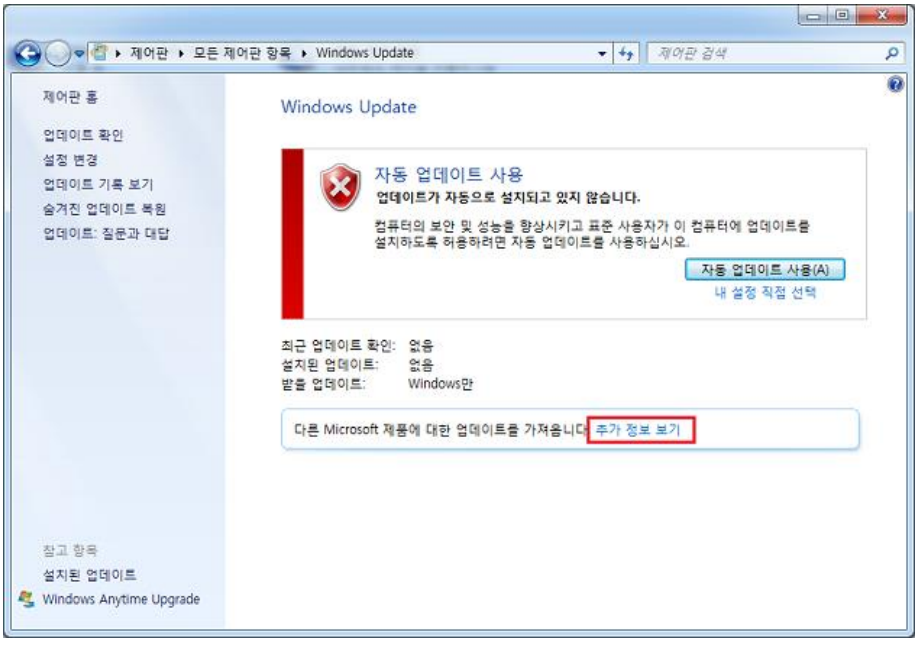
업데이트를 모두 마친 후 업데이트 사이트에 다시 접속하여 누락된 중요 업데이트가 있는지 다시 한 번 확인할 것을 권장합니다.

Windows 7

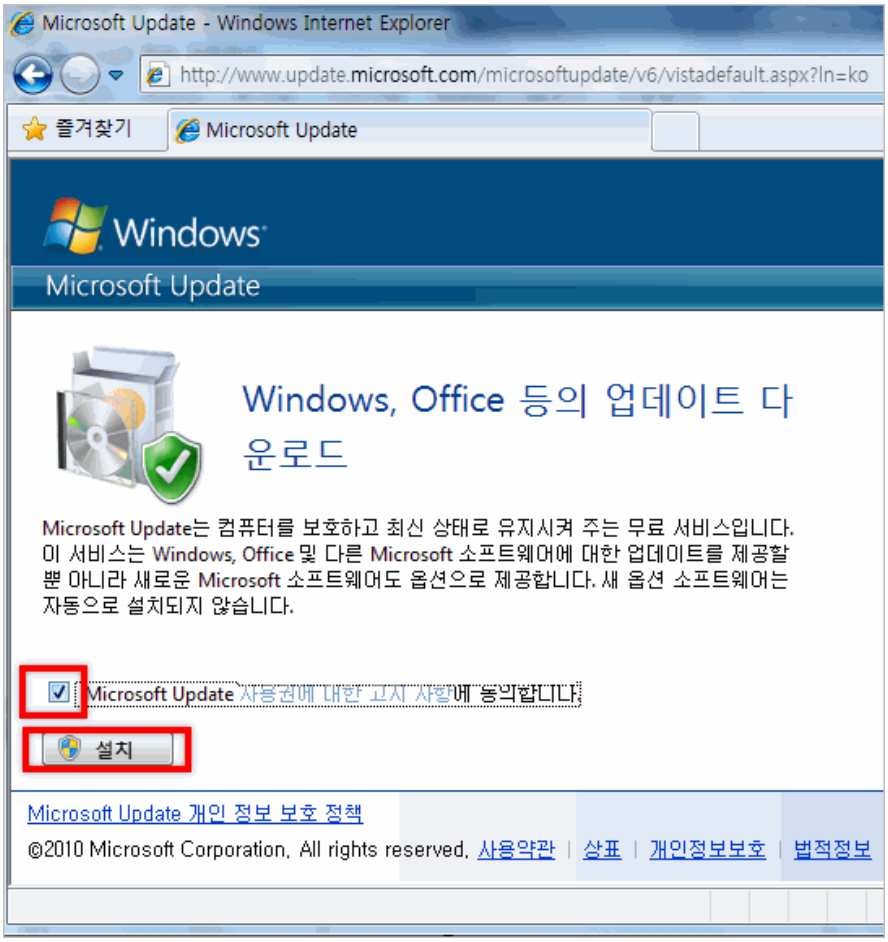
1. 작업 표시줄의 **시작** > **모든 프로그램**에서 **Windows Update**를 선택합니다.



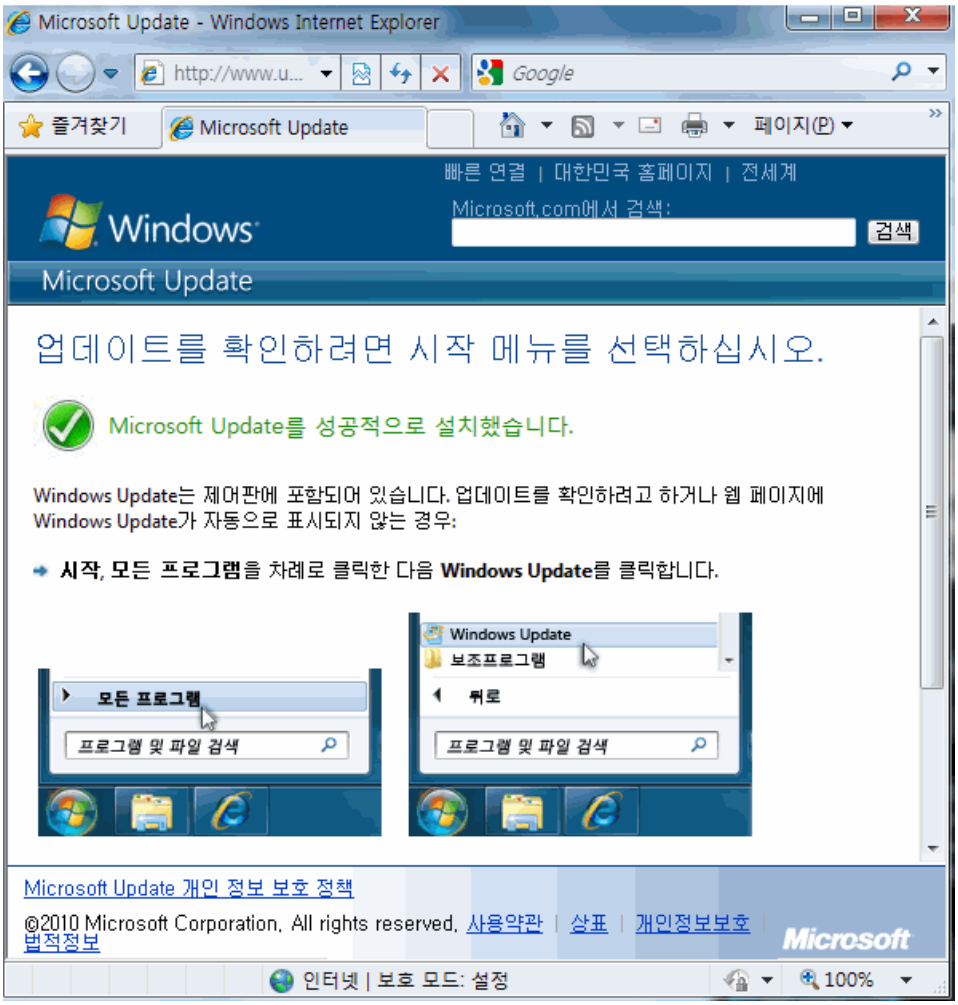
2. Windows와 MS Office에 대한 최신 업데이트를 설치하려면 **추가 정보 얻기**를 선택합니다.



3. IE가 실행되면 **Microsoft Update 사용권에 대한 고지 사항에 동의합니다** 를 선택하고 **설치**를 눌러 Microsoft Update를 실행합니다.

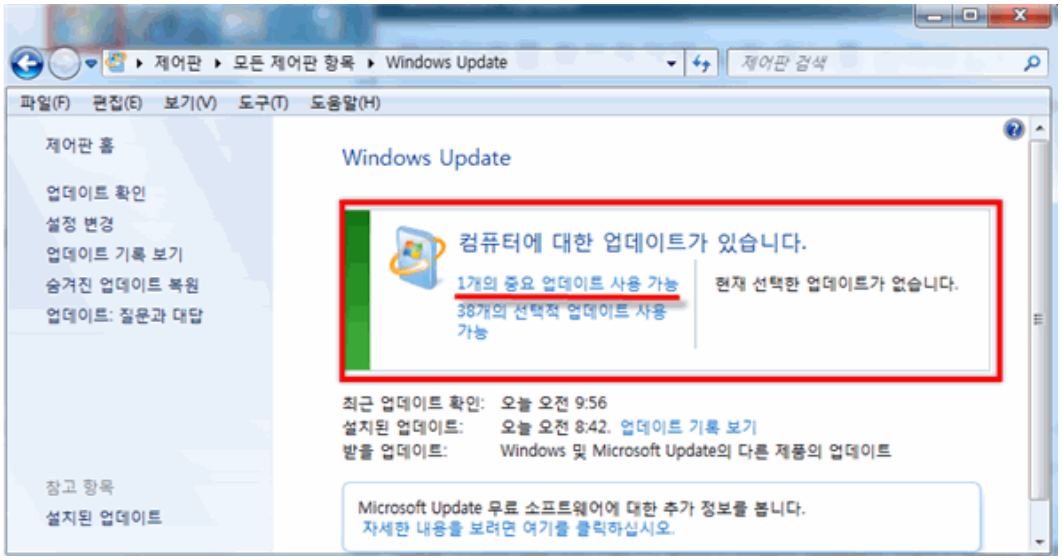


4. Microsoft Update를 마치면 다음 화면과 같이 설치 완료 알림 화면이 나타납니다.



추가 업데이트하기

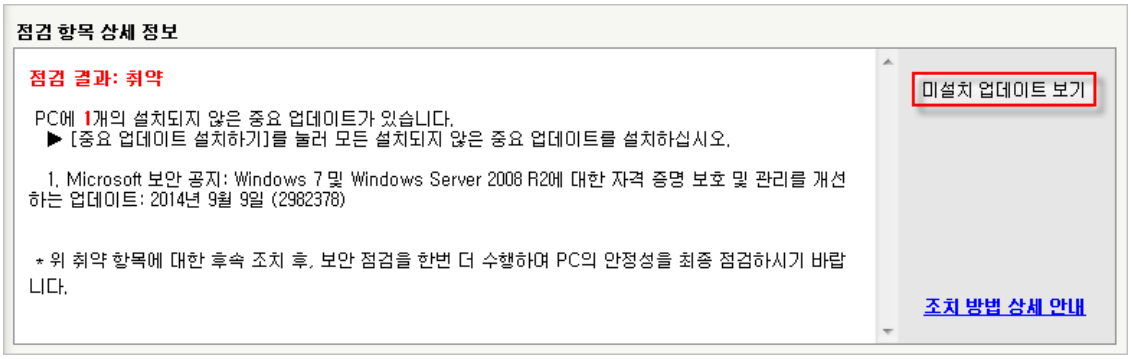
1. 작업 표시줄의 **시작** > **모든 프로그램**에서 **Windows Update**를 선택합니다.
2. 설치가 필요한 업데이트 링크를 선택하면 업데이트 설치를 시작합니다.



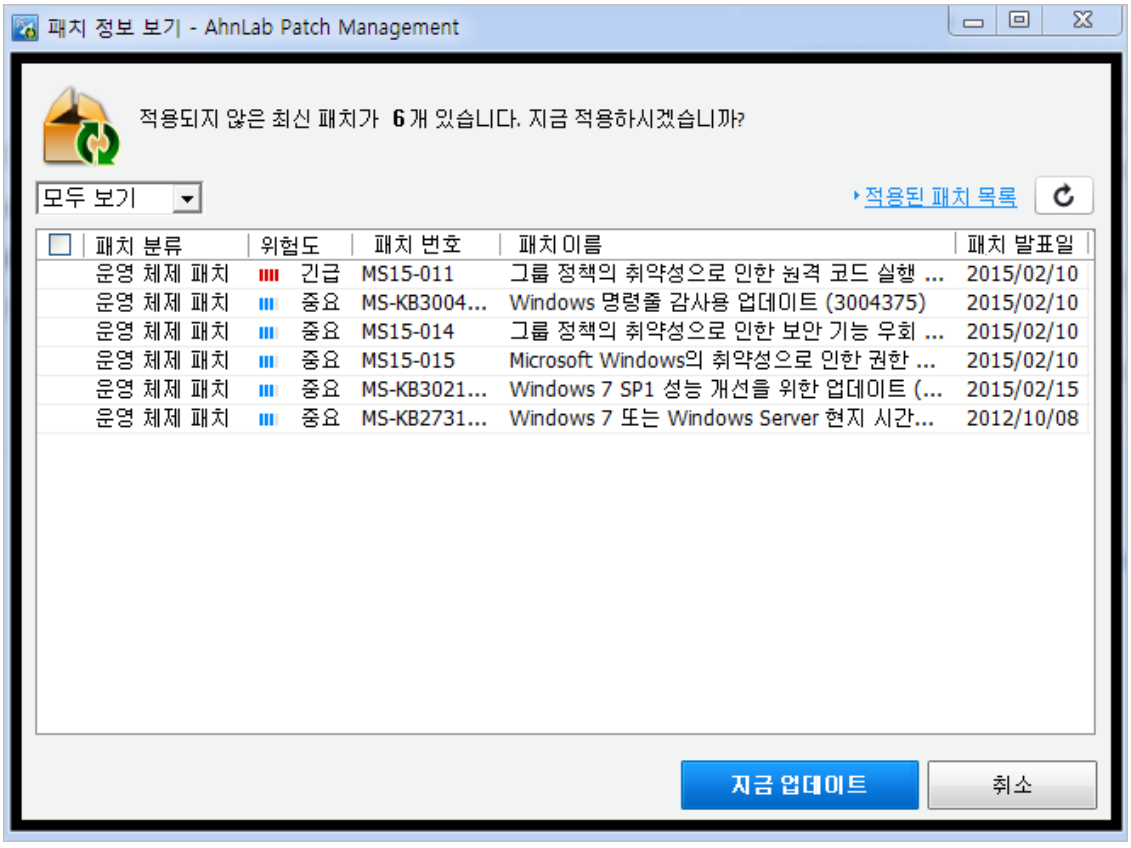
[APM 라이선스가 있는 경우]

APM 제품을 통해 적용되지 않은 패치 목록을 확인하고 최신 보안 패치를 적용할 수 있습니다.

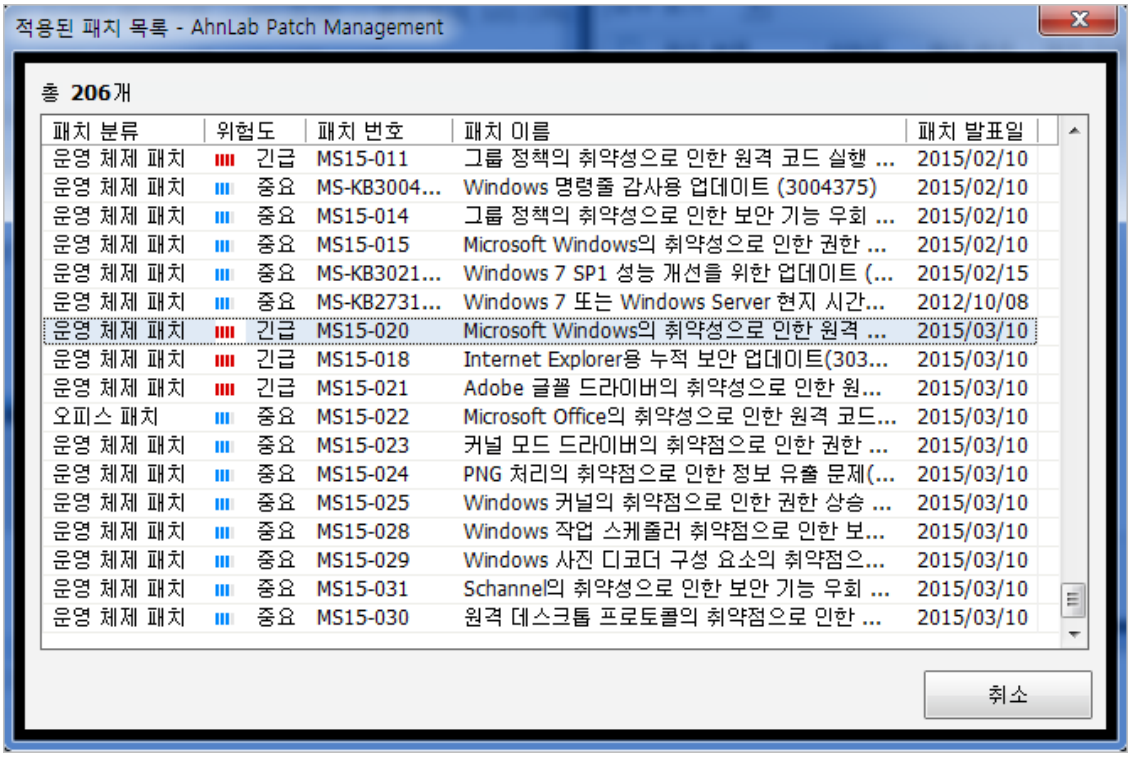
1. 미설치 업데이트 보기를 누릅니다.



2. APM이 실행되며 <패치 정보 보기>에서 현재 사용자 PC에 적용되지 않은 패치 목록을 확인할 수 있습니다.



3. **지금 업데이트**를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.
4. 패치 적용이 완료되면 화면 상단의 **적용된 패치 목록**을 눌러 설치된 패치 정보를 확인할 수 있습니다.



참고

자동 패치 시스템을 이용하는 경우 점검 결과가 PC 의 실제 보안 상태와 다르게 나타날 수 있습니다. 보안 정책에 따라 설치하지 않는 업데이트는 업데이트 숨기기를 선택하면 해당 업데이트를 점검 대상에서 제외합니다.

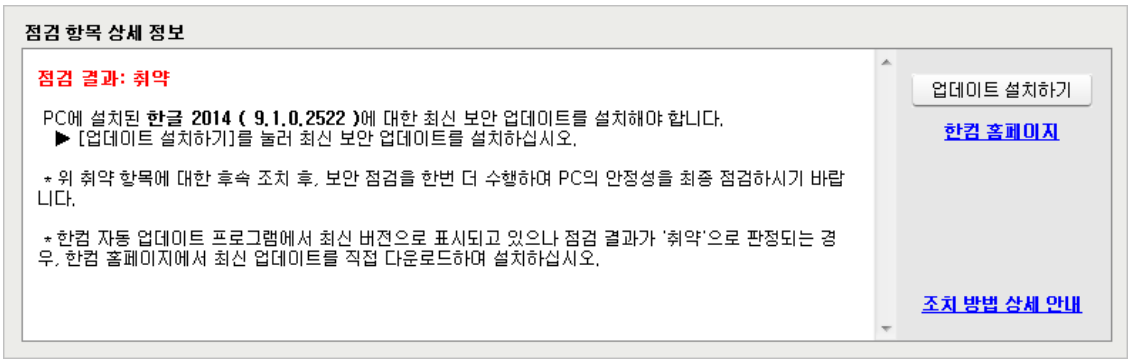
한글 프로그램의 최신 보안 패치 점검

한글 프로그램의 보안 패치 적용을 점검하여 최신 상태가 아닐 경우, 최신 보안 업데이트를 적용하도록 조치합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 의 한글 프로그램이 최신 상태입니다.
- 취약: 점검 결과가 취약으로 나오는 경우, 설치된 한글 프로그램의 버전이 표시됩니다. **업데이트 설치하기**를 눌러 최신 보안 업데이트를 설치하십시오.



참고

업데이트 설치하기를 통한 최신 보안 패치는 **한글** 프로그램에 대해서만 업데이트가 진행됩니다.
한컴오피스 2010/2014 제품의 경우, **한컴 오피스 한글**만 업데이트 대상입니다.

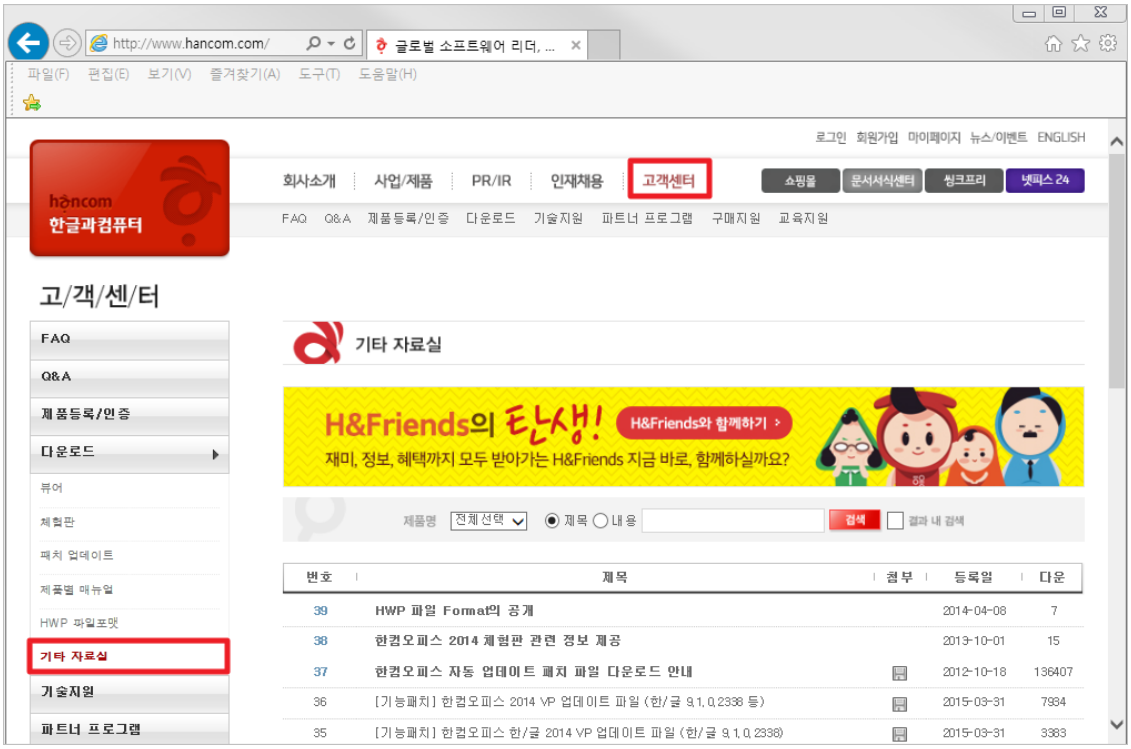
조치 방법

점검 결과가 **취약**일 때, APM 라이선스가 없는 경우와 APM 라이선스가 있는 경우에 따라 다음과 같이 조치하여 주시기 바랍니다.

[APM 라이선스가 없는 경우]

한글 2002 버전

한글 2002 버전은 한글과컴퓨터 홈페이지 > **고객센터** > **다운로드** > **기타자료실**에서 업데이트 파일을 직접 다운로드 하여 설치해야 합니다.



한/글 2004 이상의 버전

한/글 2004 이상 버전은 **시작** > **모든 프로그램** > **한글과 컴퓨터** > **한컴 자동 업데이트** 메뉴를 눌러 업데이트 파일을 다운로드 할 수 있습니다.

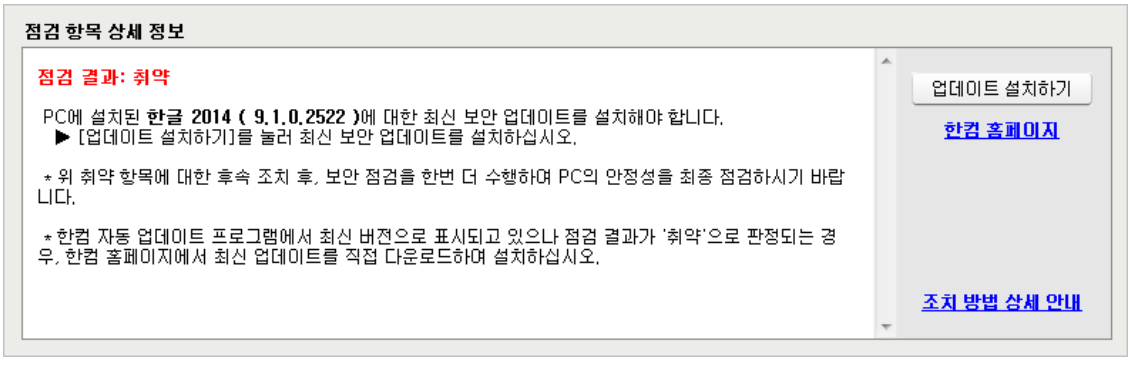
참고

한컴 자동 업데이트 프로그램에서 최신 버전으로 표시되고 있으나 내 PC 지키미 점검 결과가 '취약'으로 판정되는 경우, 한글과 컴퓨터 홈페이지에서 최신 업데이트를 다운로드 하여 설치하십시오.

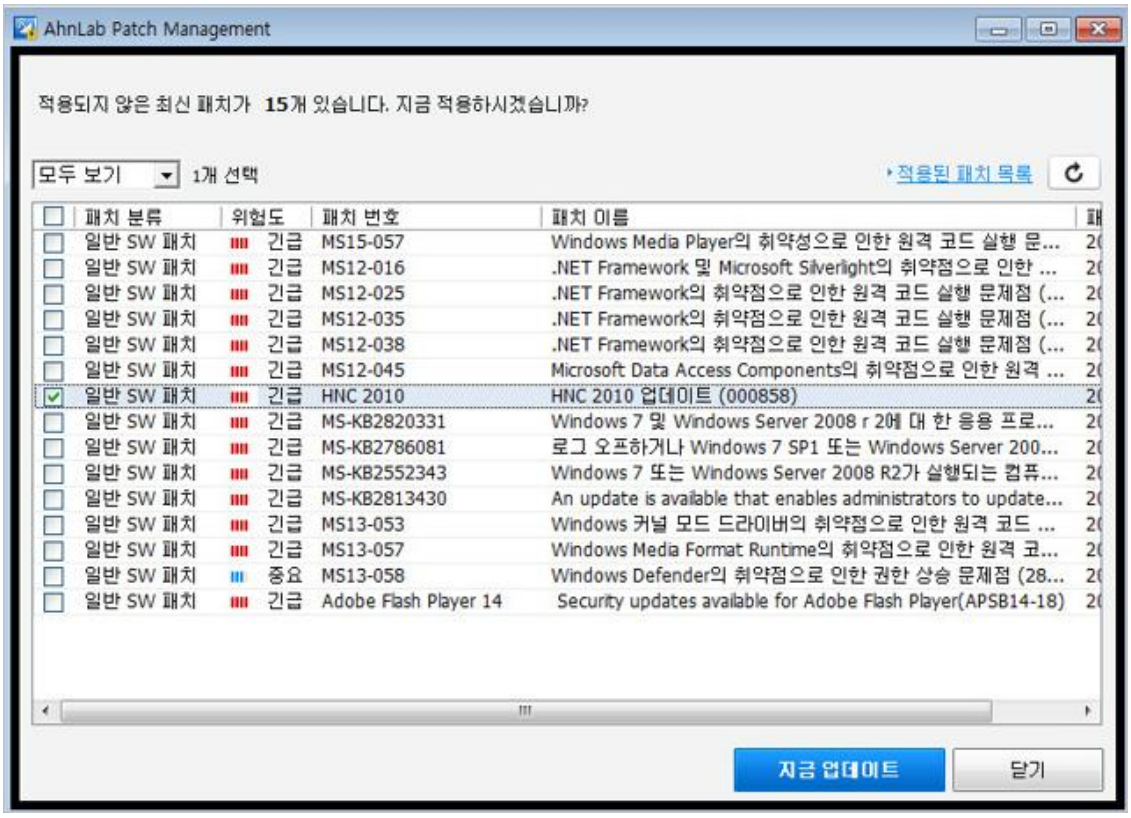
[APM 라이선스가 있는 경우]

APM 제품을 통해 적용되지 않은 패치 목록을 확인하고 최신 보안 패치를 적용할 수 있습니다.

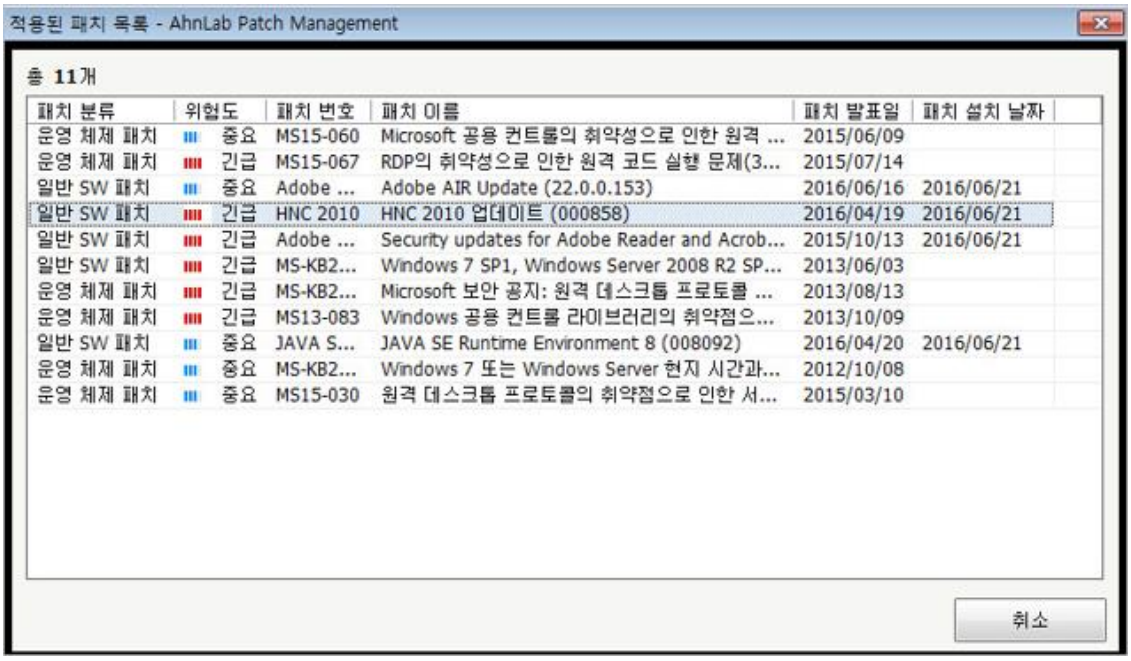
1. 미설치 업데이트 보기를 누릅니다.



2. APM이 실행되며 <패치 정보 보기>에서 현재 사용자 PC에 적용되지 않은 패치 목록을 확인할 수 있습니다.



3. **지금 업데이트**를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.
4. 패치 적용이 완료되면 화면 상단의 **적용된 패치 목록**을 눌러 설치된 패치 정보를 확인할 수 있습니다.



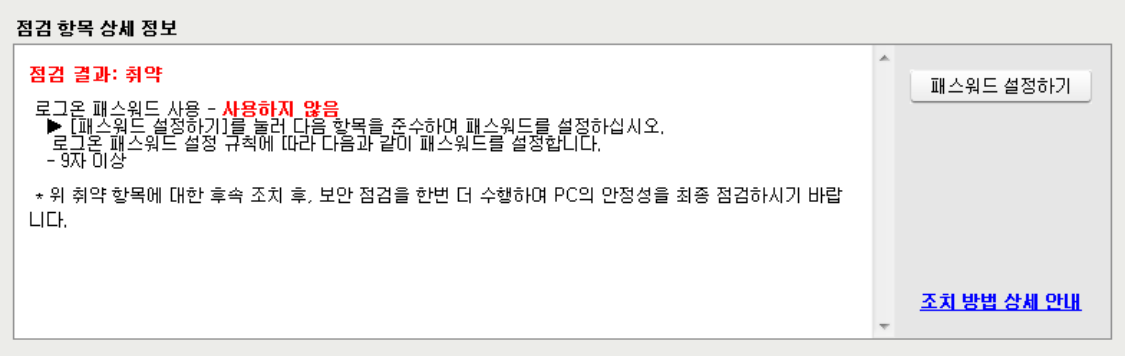
로그온 패스워드 안전성 점검

Windows 로그온 패스워드의 안전성을 점검합니다. Windows 로그온 패스워드는 Windows 로그온 시에 입력하는 패스워드입니다.

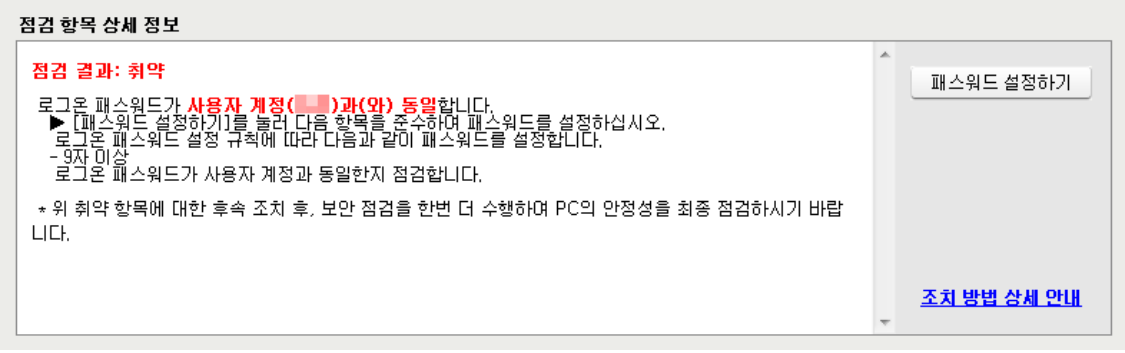
점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

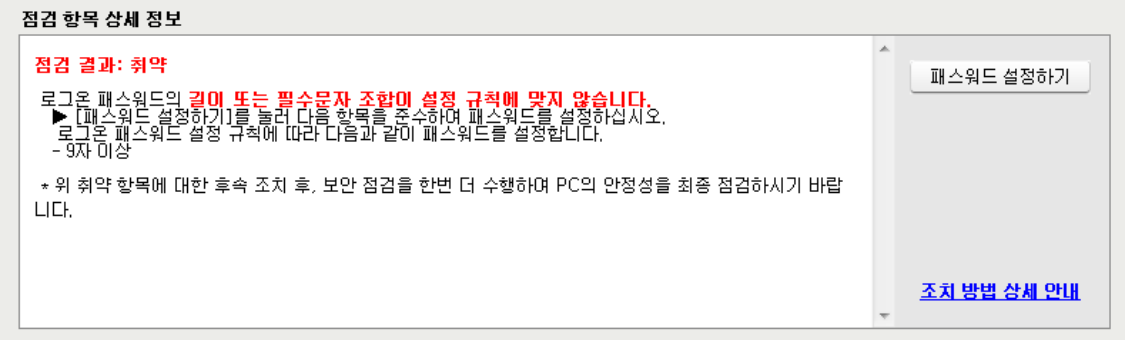
- 안전: PC 의 로그온 패스워드가 안전성을 모두 만족하는 경우입니다.
- 취약: 점검 결과가 취약으로 나오는 경우, 로그온 패스워드 안전성 점검에 대한 상세 결과를 나타냅니다.
  - 로그온 패스워드 사용이 **사용하지 않음**으로 나타납니다. **패스워드 설정하기**를 눌러 패스워드를 재설정하거나 **시작** > **제어판** > **사용자 계정**을 선택하고, Windows 로그온 패스워드를 설정합니다.



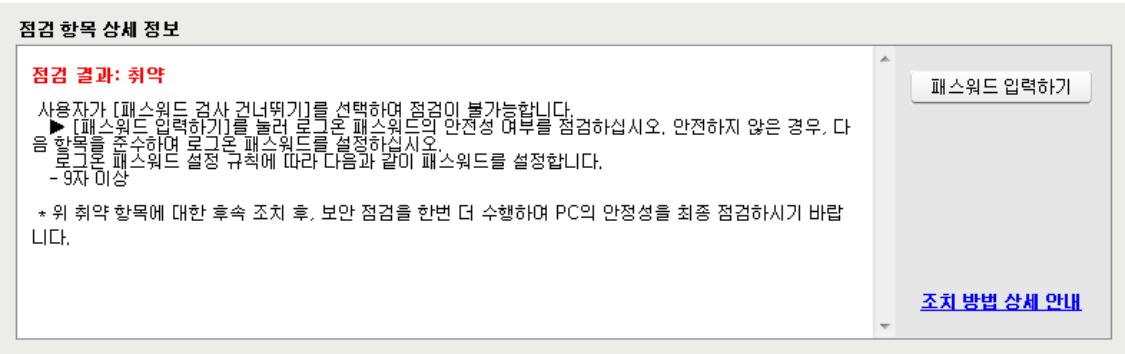
  - 로그온 패스워드가 **사용자 계정과 동일**한 것으로 나옵니다. **패스워드 설정하기**를 누르거나 **시작** > **제어판** > **사용자 계정**을 선택하고, 사용자 계정에 사용된 문자열과 동일하지 않은 로그온 패스워드를 설정합니다.



  - 로그온 패스워드의 **길이 또는 필수문자 조합**이 안전 조건을 준수하지 않는 것으로 나타납니다. **패스워드 설정하기**를 누르거나 **시작** > **제어판** > **사용자 계정**을 선택하고, 패스워드의 길이와 필수문자 조합이 안전 조건을 준수하도록 패스워드를 설정합니다.



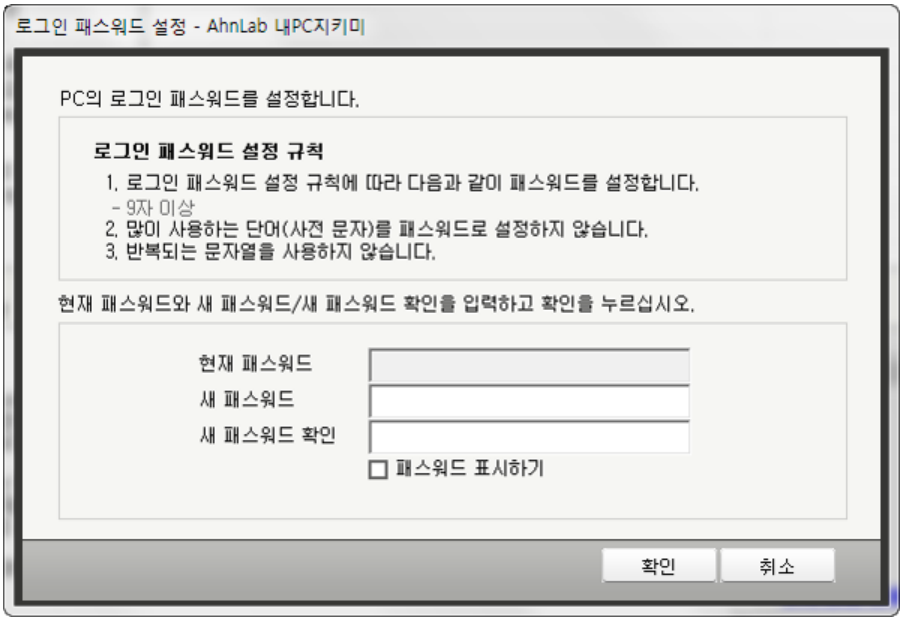
- 로그온 패스워드를 점검하지 않고, **패스워드 검사 건너뛰기**를 한 경우입니다. **패스워드 입력하기**를 누르거나 **시작** > **제어판** > **사용자 계정**을 선택하고 Windows 로그온 패스워드를 다음의 안전 조건을 준수하여 설정합니다.



패스워드 설정하기

패스워드 안전성 점검 결과 확인 후 패스워드 설정하기를 누르면 <로그온 패스워드 설정>이 나타납니다.

- 현재 패스워드: 현재 사용 중인 로그온 패스워드를 입력합니다.
- 새 패스워드: 변경할 새 패스워드를 입력합니다
- 새 패스워드 확인: 새 패스워드 입력란에 입력한 패스워드와 동일한 패스워드를 다시 입력합니다.



조치 방법

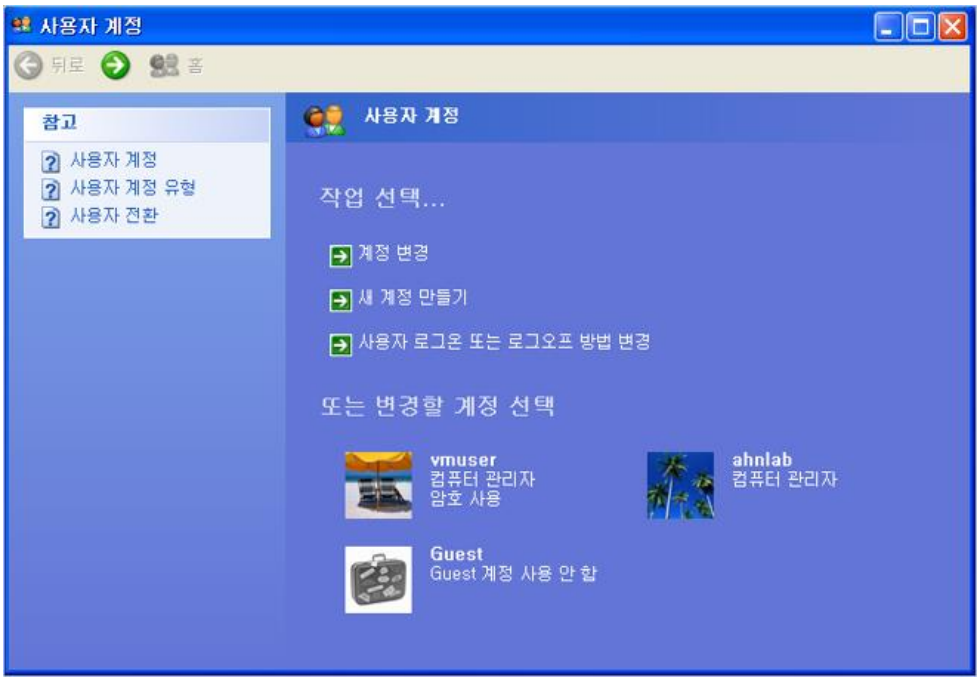
Windows 로그온 패스워드 설정 방법은 다음과 같습니다.

참고

새로 입력하는 Windows 로그온 패스워드는 다음의 조건을 만족해야 합니다.
- 사용자 계정(ID)의 문자열과 일치하지 않는 패스워드
- 길이 및 필수문자 조합이 안전 조건을 준수하는 패스워드
- 패스워드 안전성 검사 결과 '안전'인 패스워드

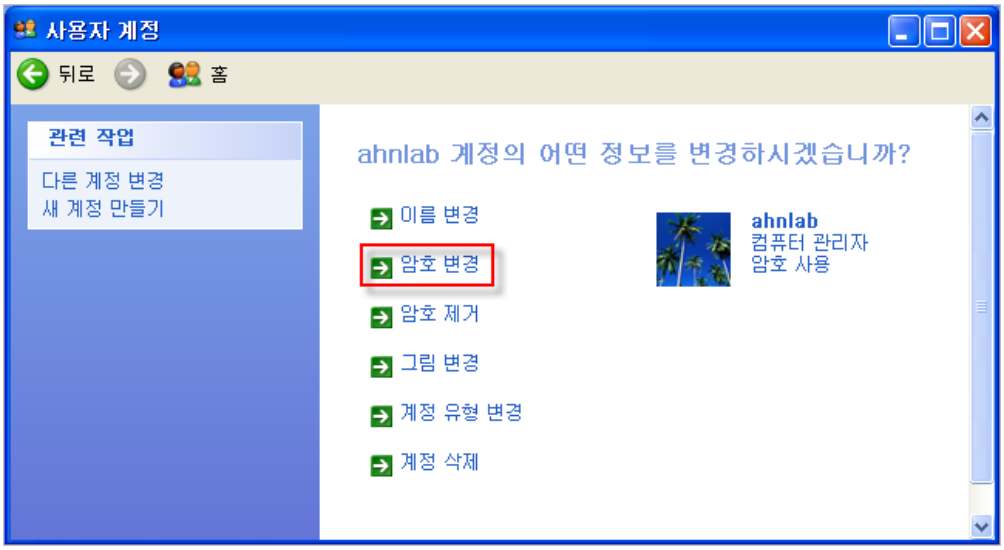
Windows XP

1. **시작** > **설정** > **제어판**을 선택한 후 제어판이 나타나면 **클래식 보기**로 전환합니다.
2. 사용자 계정을 선택합니다.
3. 사용자 계정 목록에서 패스워드를 변경할 계정을 선택합니다.



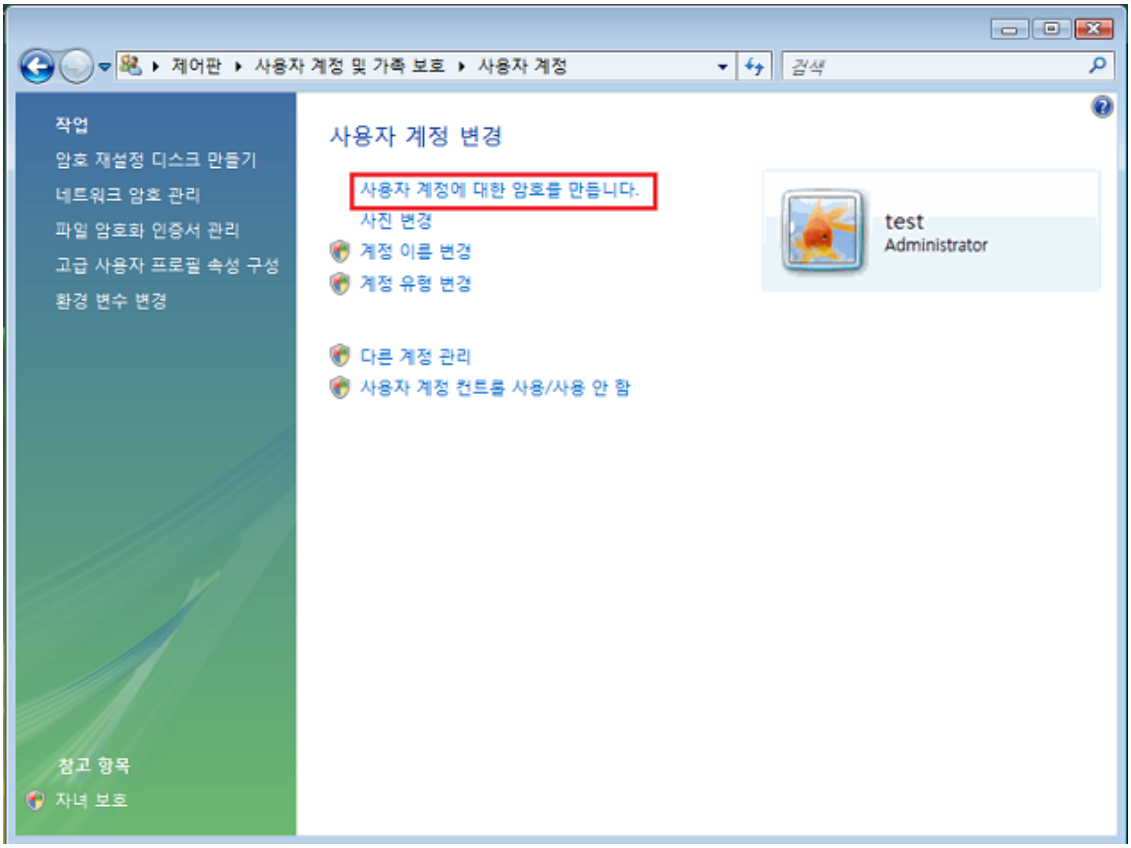
4. ***계정의 어떤 정보를 변경하시겠습니까? 라는 메시지 창이 나타나면 경우에 따라 다음과 같이 선택합니다.
   - 패스워드가 없는 경우: **암호 만들기**를 선택합니다.

- 기존 패스워드가 있는 경우: **암호 변경**을 선택합니다.

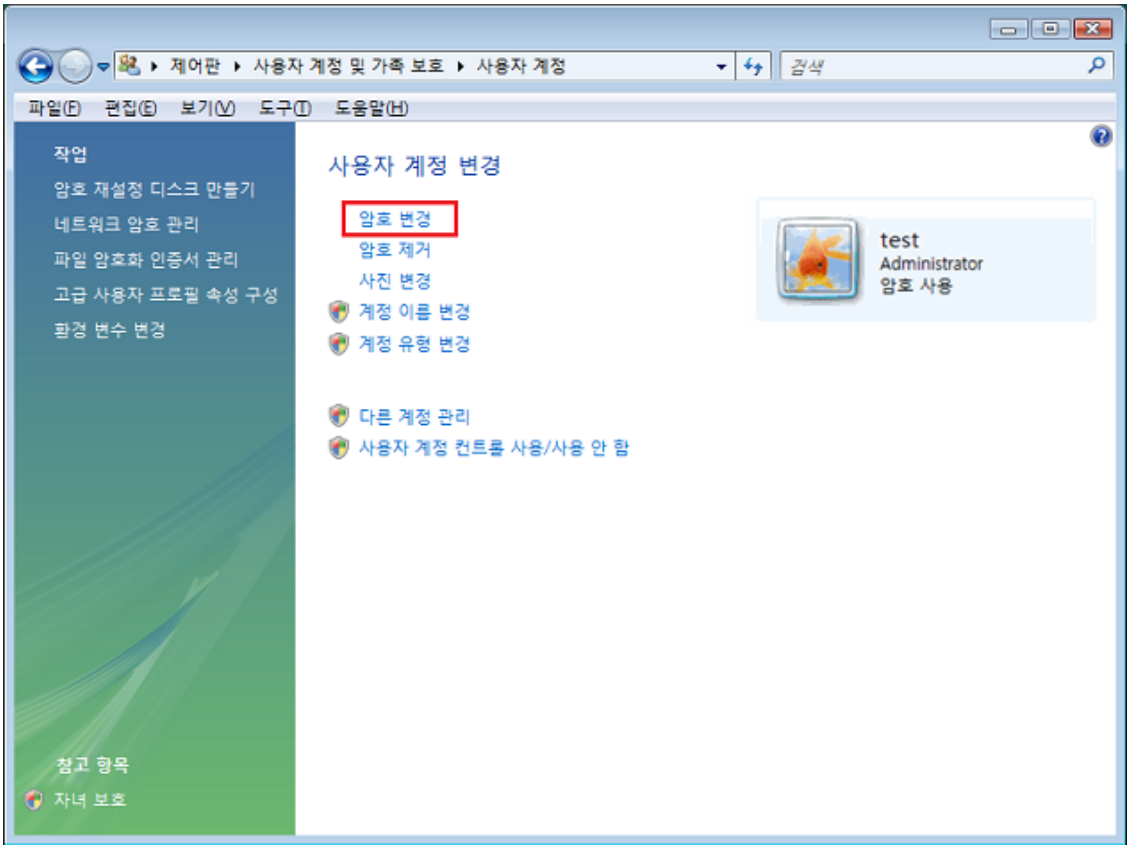


Windows Vista

1. **시작** > **설정** > **제어판**을 선택한 후 제어판이 나타나면 **클래식 보기**로 전환합니다.
2. 사용자 계정을 선택합니다.
3. 패스워드가 없는 경우 다음 화면에서 **사용자 계정에 대한 암호를 만듭니다**를 선택합니다.

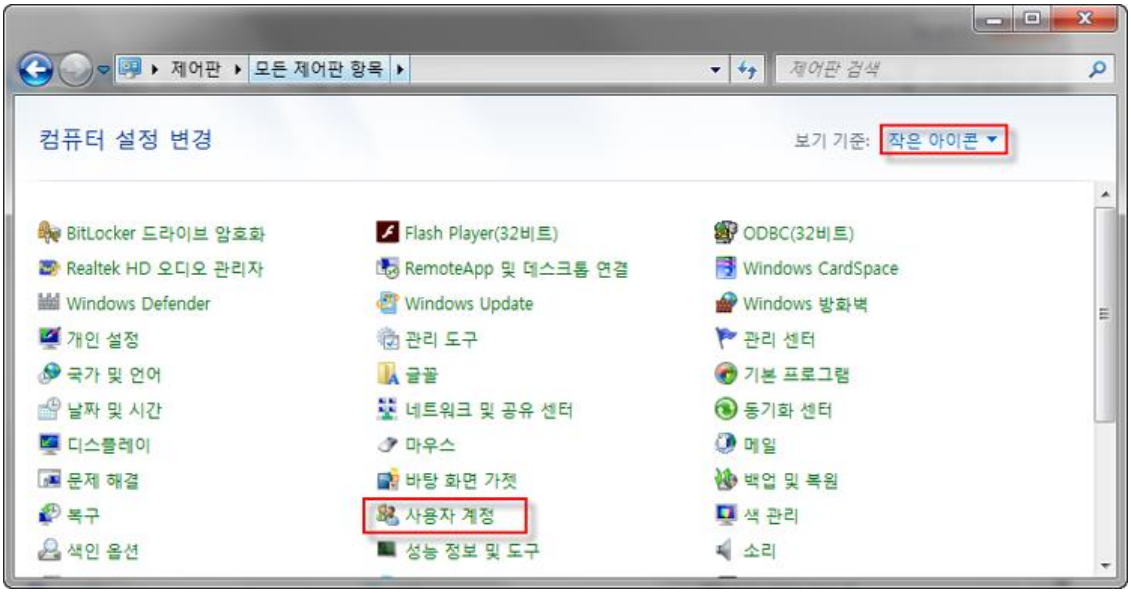


4. 패스워드를 변경하려면 다음 화면에서 **암호 변경**을 선택합니다.

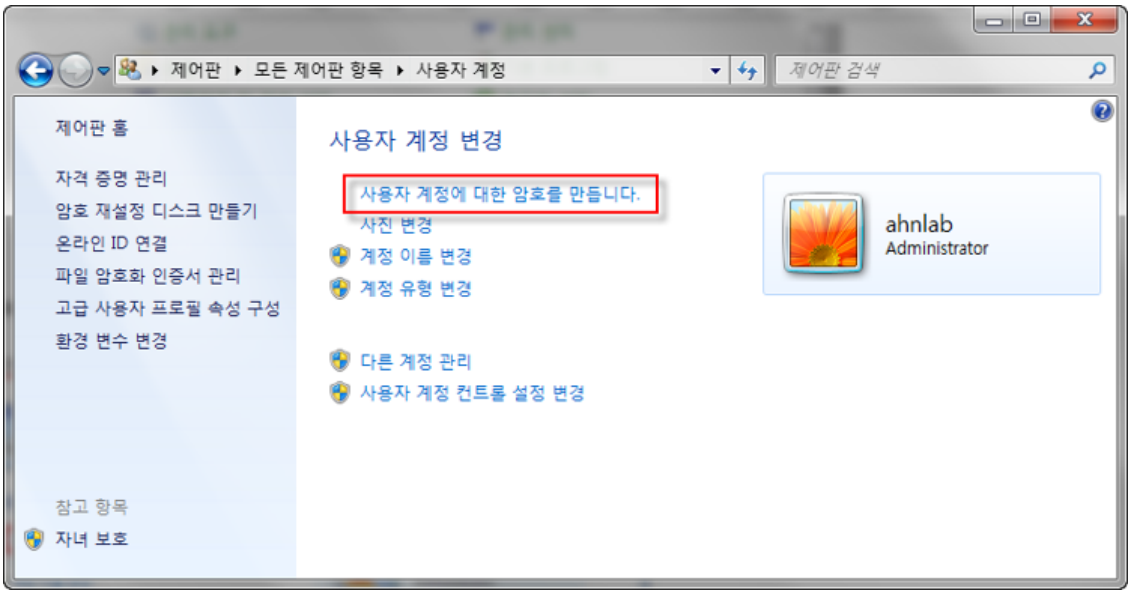


Windows 7

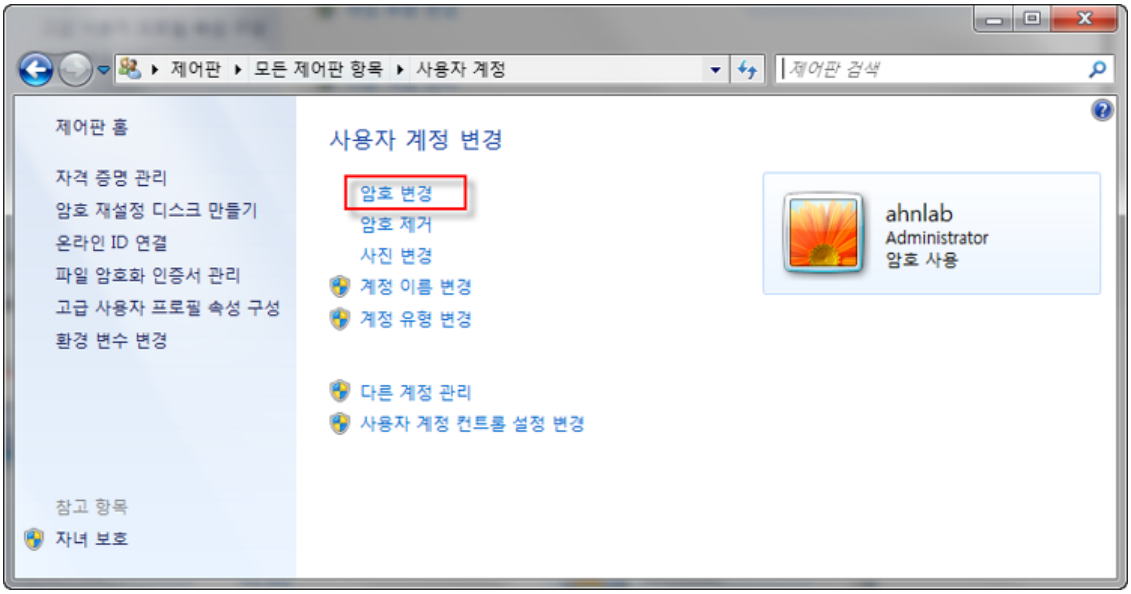
1. **시작** > **제어판** 실행 후 **작은 아이콘 보기**로 전환하고 **사용자 계정**을 선택합니다.



2. 패스워드가 없는 경우 다음 화면에서 **사용자 계정에 대한 암호를 만듭니다**를 선택합니다.



3. 패스워드를 변경하려면 다음 화면에서 **암호 변경**을 선택합니다.


제어판 ▸ 모든 제어판 항목 ▸ 사용자 계정
제어판 검색
제어판 홈
자격 증명 관리
암호 재설정 디스크 만들기
온라인 ID 연결
파일 암호화 인증서 관리
고급 사용자 프로필 속성 구성
환경 변수 변경
참고 항목
자녀 보호
사용자 계정 변경
암호 변경
암호 제거
사진 변경
계정 이름 변경
계정 유형 변경
다른 계정 관리
사용자 계정 컨트롤 설정 변경
ahnlab
Administrator
암호 사용

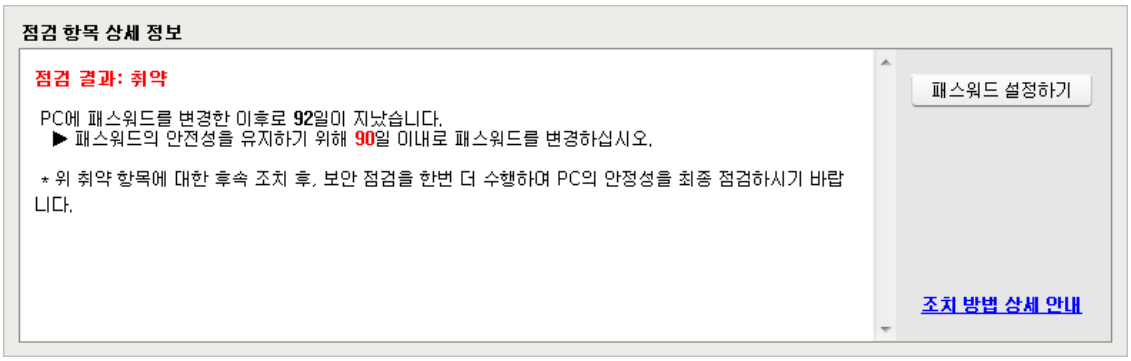
로그온 패스워드 사용 기간 점검

Windows 로그온 패스워드 사용 기간이 관리자가 설정한 기간을 경과하였는 지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

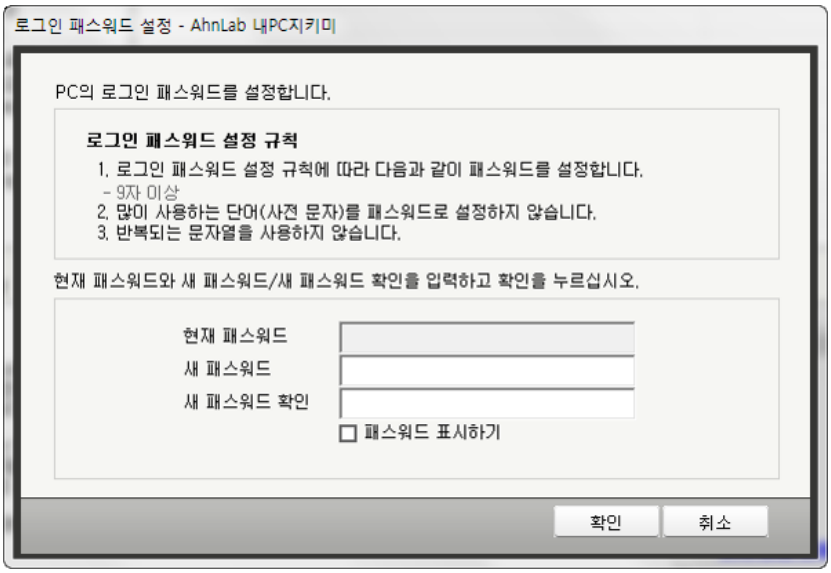
- 안전: Windows 로그온 패스워드 사용 기간이 관리자가 설정한 사용 기간을 경과하지 않았습니다.
- 취약: 점검 결과가 취약으로 나오는 경우, 로그온 패스워드 사용 기간 점검에 대한 상세 결과를 나타냅니다.
- PC 에 로그온 패스워드를 변경한 이후로 경과한 날짜를 나타냅니다. **패스워드 설정하기**를 누르거나 **시작 > 제어판 > 사용자 계정**을 선택하고, Windows 로그온 패스워드를 설정합니다.



조치 방법

로그온 패스워드를 설정하는 방법은 다음과 같습니다. 패스워드 안전성 점검 결과 확인 후 **패스워드 설정하기**를 누르면 <로그온 패스워드 설정>이 나타납니다.

- 현재 패스워드: 현재 사용 중인 로그온 패스워드를 입력합니다
- 새 패스워드: 변경할 새 패스워드를 입력합니다
- 새 패스워드 확인: 새 패스워드 입력란에 입력한 패스워드와 동일한 패스워드를 다시 입력합니다.



참고

Windows 의 패스워드 변경 기능을 직접 실행하려면 로그온 패스워드 안전성 점검을 참고하십시오.

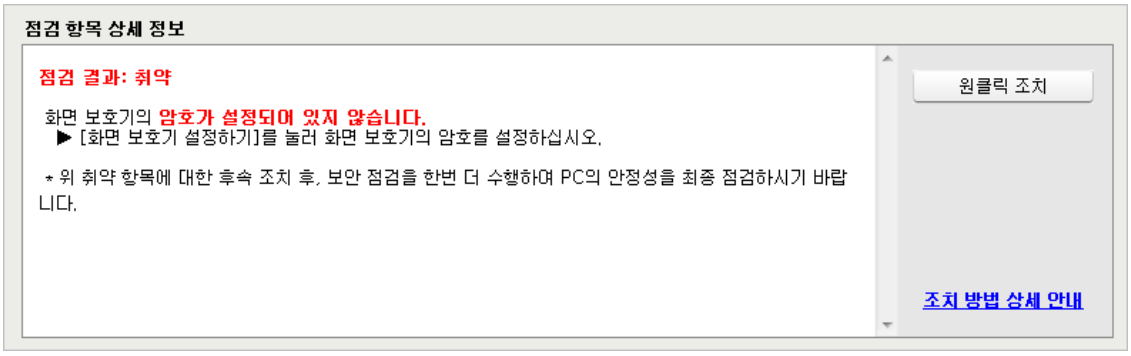
화면 보호기 설정 점검

화면 보호기의 설정 값들을 점검합니다. 자리를 비울 경우에는 다른 사용자의 PC 접근으로 인한 정보 유출을 방지하기 위해 화면 보호기 설정과 화면 보호기의 패스워드를 반드시 설정해야 합니다.

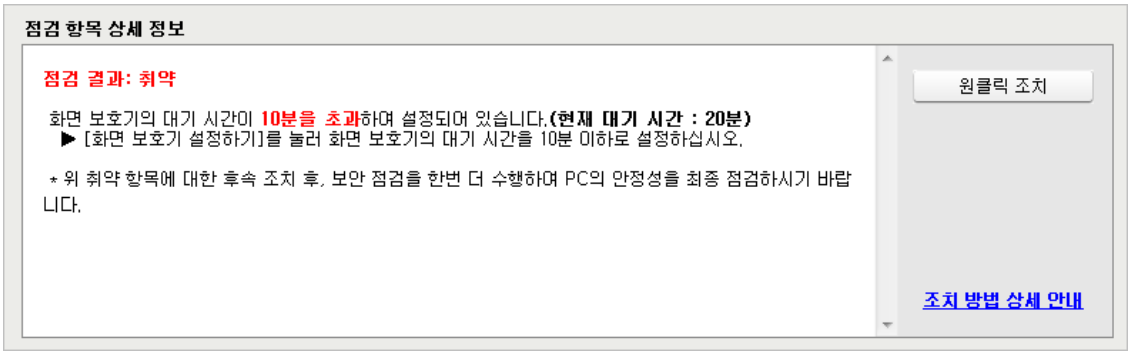
점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

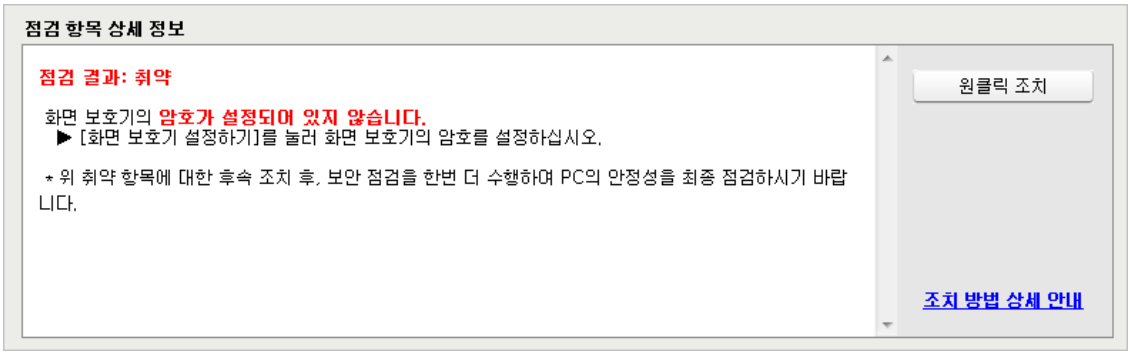
- 안전: PC 에 화면 보호기가 설정이 안전하게 설정되어 있습니다. PC 에 화면 보호기를 사용하도록 설정되어 있고, 대기 시간이 관리자가 설정한 시간 내로 설정되어 있으며 화면 보호기 종료 시에 패스워드를 입력하도록 설정되어 있습니다.
- 취약: 점검 결과가 취약으로 나오는 경우, 화면 보호기 설정 점검에 대한 상세 결과를 나타냅니다.
  - 화면 보호기가 비활성화 되어 있는 경우: **원클릭 조치**를 눌러 화면 보호기를 설정합니다.



  - 화면 보호기 대기 시간이 관리자가 지정한 시간 이상인 경우: **원클릭 조치**를 눌러 대기 시간을 관리자가 지정한 설정 값으로 설정합니다.



  - 화면 보호기의 비밀번호가 설정되어 있지 않은 경우: **원클릭 조치**를 눌러 제어판의 화면 보호기 설정 화면에서 **다시 시작할 때 암호로 보호**를 선택합니다.



조치 방법

Windows XP

1. **시작** > **제어판**에서 **디스플레이**를 선택합니다.
2. <디스플레이 등록 정보>에서 화면 보호기 탭을 선택합니다.
3. 화면 보호기 설정 탭에서 다음의 내용을 설정합니다.
   - 원하는 화면 보호기의 모양을 선택합니다.
   - 대기: 시간을 관리자가 지정한 시간으로 설정합니다.
   - **다시 시작할 때 암호로 보호**를 선택합니다.

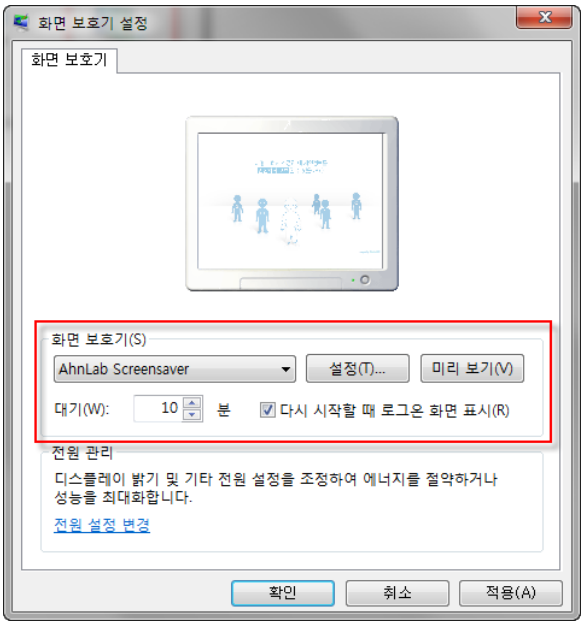
4. **확인**을 누릅니다.

Windows Vista / Windows 7

1. 바탕 화면에서 마우스 오른쪽을 누르고 **개인 설정**을 선택합니다.

2. <개인 설정>에서 **화면 보호기**를 선택합니다.

3. 화면 보호기 설정 화면에서 다음의 내용을 설정합니다.
   - 원하는 화면 보호기를 선택합니다.
   - 대기: 대기 시간을 관리자가 지정한 시간 이하로 설정합니다.
   - **다시 시작할 때 로그온 화면 표시**를 선택합니다.



4. **확인**을 누릅니다.

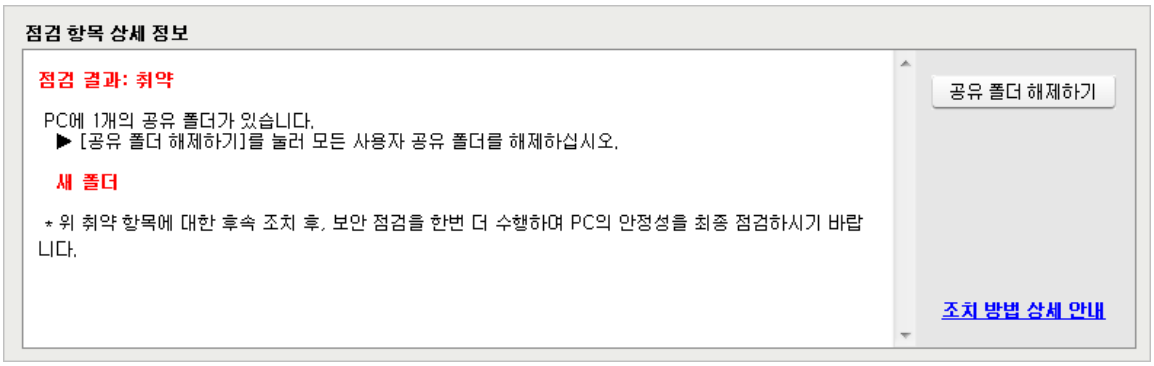
사용자 공유 폴더 설정 점검

사용자 공유 폴더가 설정되어 있는지 점검합니다. 최근 악성코드는 공유 폴더를 이용하여 확산되는 경우가 많으므로 공유 폴더는 가능한 사용하지 않는 것이 좋습니다. ADMIN$,C$, D$, IPC$, PRINT$와 같은 관리자 공유 폴더는 점검 대상에 포함되지 않으며 사용자가 직접 설정한 사용자 공유 폴더에 대해서만 점검 결과를 표시합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

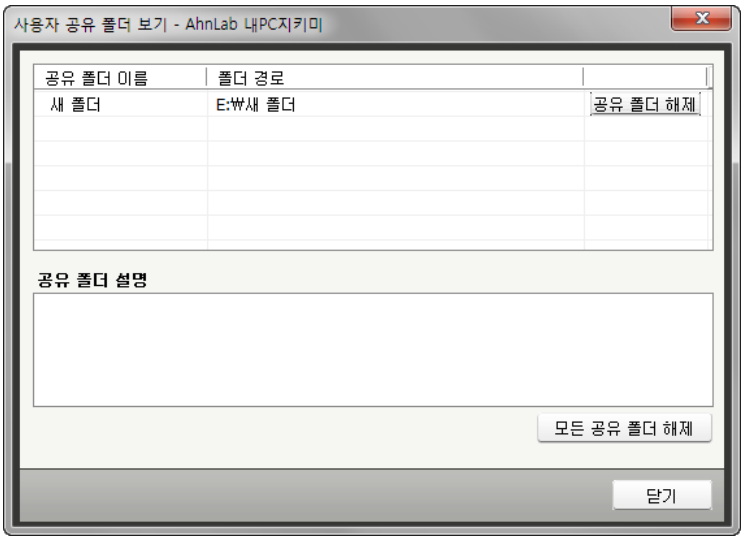
- 안전: PC 에 사용자 공유 폴더가 설정되어 있지 않습니다.
- 취약: 점검 결과가 취약으로 나오는 경우, 사용자 공유 폴더 설정 점검에 대한 상세 결과를 나타냅니다.
  - PC 에 설정 되어있는 공유 폴더 개수를 나타냅니다. **공유 폴더 해제하기**를 눌러 모든 사용자 공유 폴더를 해제하십시오.



조치 방법

점검 결과가 **취약**인 경우 다음과 같이 조치하여 주시기 바랍니다.

1. 점검 항목 상세 정보에서 **공유 폴더 해제하기**를 누릅니다.
2. <사용자 공유 폴더 보기>에서 공유 폴더 목록이 표시됩니다. **공유 폴더 해제** 또는 **모든 공유 폴더 해제**를 누르면 설정되어 있는 공유 폴더가 해제됩니다.



- 공유 해제: 선택한 폴더의 공유를 해제합니다.
- 모든 공유 폴더 해제: 설정되어 있는 모든 공유 폴더의 공유를 해제합니다.

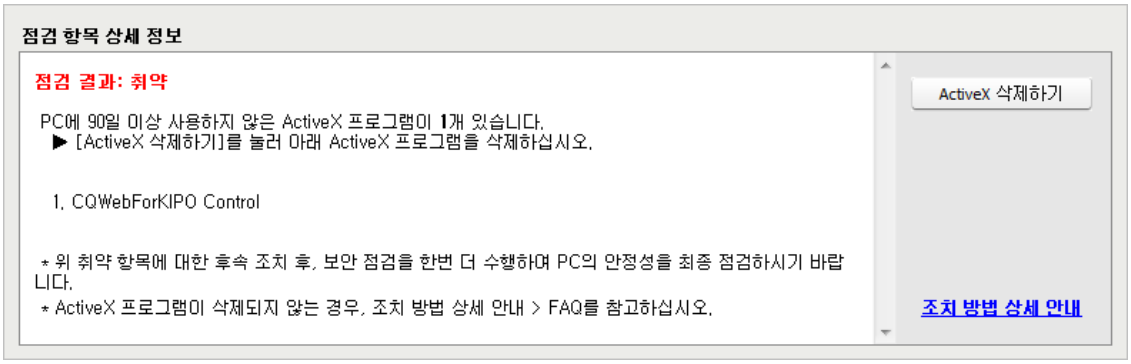
미사용 ActiveX 프로그램 점검

관리자가 설정한 기간이 지나도록 사용하지 않은 ActiveX 프로그램이 있는지 점검합니다. ActiveX 는 각종 인터넷 사이트 접속 시에 해당 웹 페이지 표시를 위해 주로 설치되며, 해당 ActiveX 프로그램을 더 이상 사용하지 않는 경우에는 가능한 삭제하는 것이 좋습니다. 보안에 취약한 ActiveX 프로그램은 악의적인 사용자에 의해 해킹에 악용될 우려가 있습니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 관리자가 설정한 기간 이상 사용하지 않은 Active X 프로그램이 존재하지 않습니다.
- 취약: PC 에 관리자가 설정한 기간 이상 사용하지 않은 Active X 프로그램의 개수를 나타냅니다. **ActiveX 삭제하기**를 눌러 사용하지 않는 Active X 를 삭제합니다.



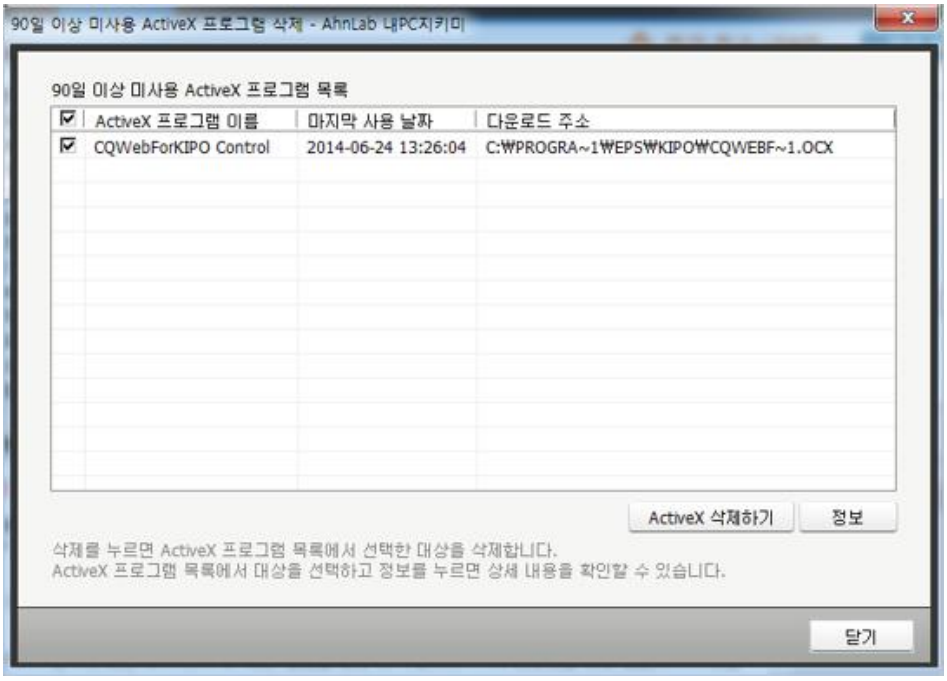
참고

ActiveX 프로그램 삭제 시에는 내 PC 지키미 담당자에게 문의하시기 바랍니다. 또한, 꼭 필요한 사이트의 ActiveX 인 경우에는 해당 사이트에 접속하면 다시 설치됩니다.

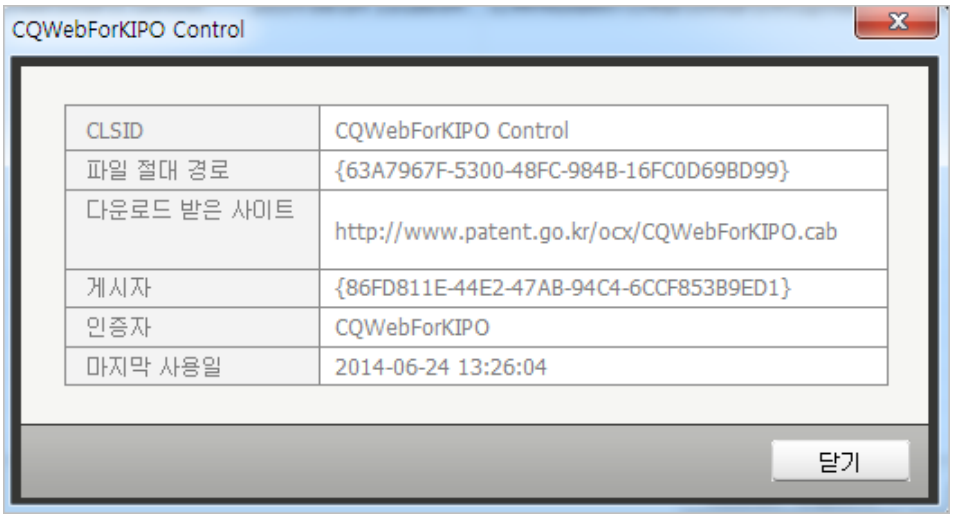
조치 방법

ActiveX 삭제하기를 실행하면 설치된 ActiveX 목록 중 관리자가 설정한 기간 이상 사용하지 않은 ActiveX 목록을 확인할 수 있습니다. 사용자는 ActiveX 목록에서 필요 없는 항목을 직접 선택하여 삭제하거나 설치된 ActiveX 에 대한 상세 정보를 확인할 수 있습니다.

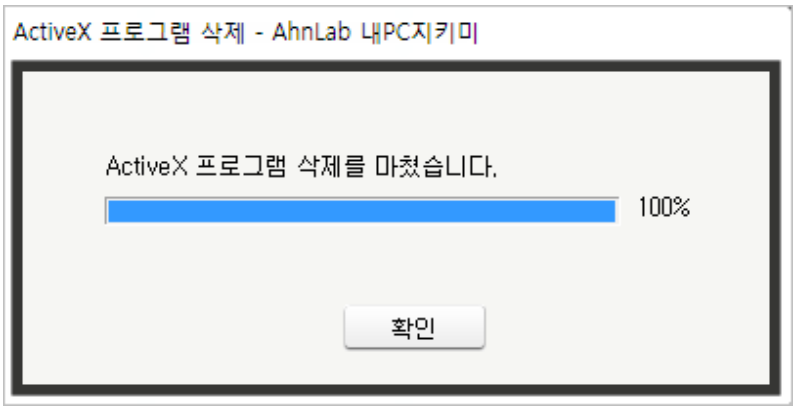
1. 미사용 ActiveX 프로그램 존재 점검 항목에서 취약으로 진단된 경우 점검 항목 상세 정보 옆에 있는 **ActiveX 삭제하기**를 실행합니다.
2. 미사용 ActiveX 프로그램 목록이 화면에 나타납니다. 목록에서 삭제할 대상을 선택한 후에 **ActiveX 삭제하기**를 누릅니다.



- ActiveX 프로그램 목록에 표시된 ActiveX 에 대한 상세 정보를 확인하고 싶으면 정보를 누릅니다.



3. 삭제 진행 과정이 표시되며, 삭제가 완료되면 **확인**을 눌러 창을 닫습니다.



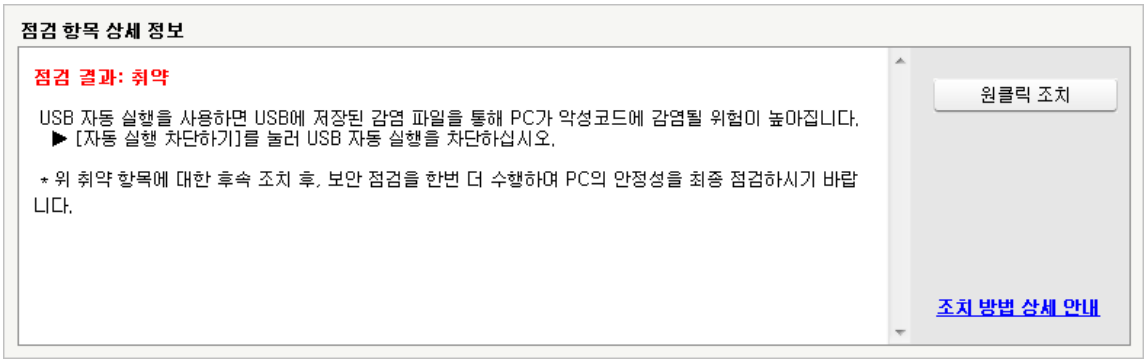
USB 자동 실행 설정 점검

USB 미디어를 PC 에 연결했을 때 USB 안의 파일이 자동 실행하도록 설정되어 있는 지 점검합니다. 최근의 악성코드는 USB 자동 실행 기능을 이용하여 PC 에 악성코드를 유포하는 방법을 사용하고 있습니다. 따라서, USB 가 자동 실행되도록 설정되어 있으면 악성코드에 감염 위험이 높아질 수 있으므로 USB 자동 실행을 허용하지 않는 것이 좋습니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 USB 가 연결되었을 때, USB 안의 파일들이 자동으로 실행되지 않도록 설정되어 있습니다.
- 취약: USB 가 PC 에 연결될 때 USB 안의 파일이 자동으로 실행되도록 설정되어 있습니다. **원클릭 조치**를 USB 자동 실행 기능을 해제하십시오.



참고

다른 USB 자동 실행 차단 프로그램을 설치하여 운영하고 있는 경우 점검 결과가 실제 PC 상태와 다르게 나타날 수 있습니다.

조치 방법

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. USB 자동 실행 차단이 설정되면 다음과 같은 알림 창이 나타납니다.

3. 알림 창에서 **확인**을 누릅니다. 점검 결과는 안전으로 변경됩니다.

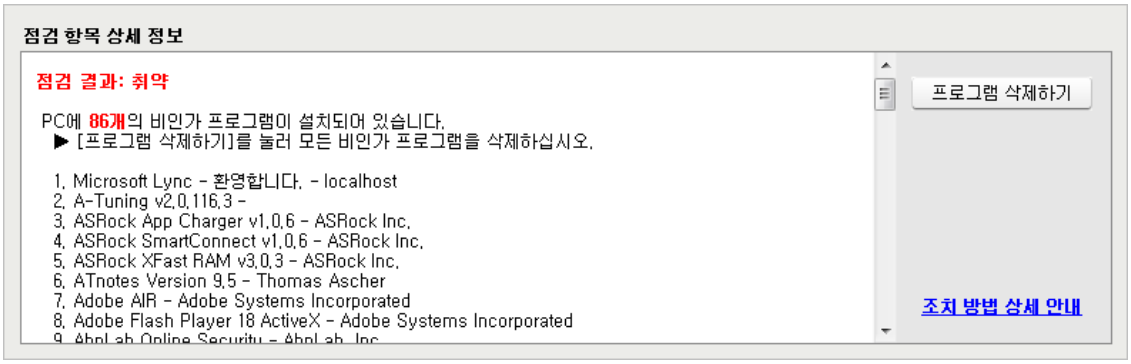
비인가 프로그램 설치 점검

사용이 허락되지 않은 비인가 프로그램의 설치 여부를 점검합니다. 비인가 프로그램이 PC 에 설치되어 있는 경우 해당 프로그램은 모두 삭제하시기 바랍니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

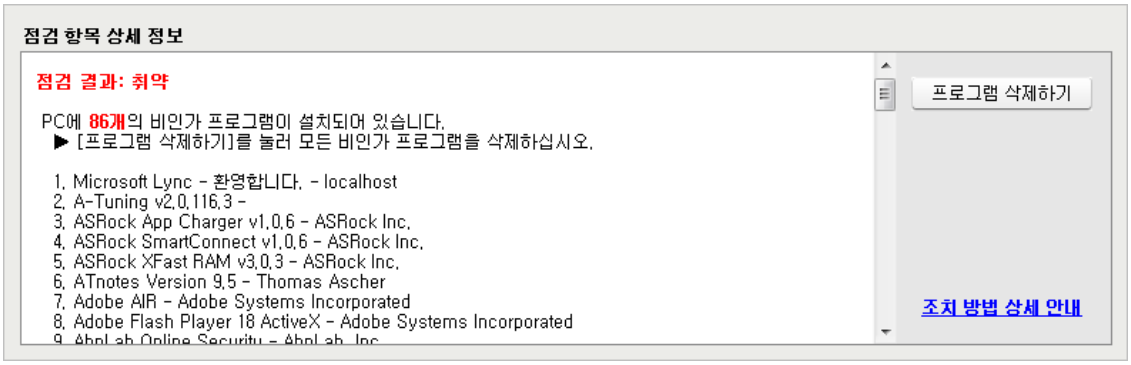
- 안전: PC 에 비인가 프로그램이 설치되어 있지 않습니다.
- 취약: PC 에 설치된 비인가 프로그램의 목록이 나타납니다. **프로그램 삭제하기**를 눌러 비인가 프로그램을 삭제하십시오.



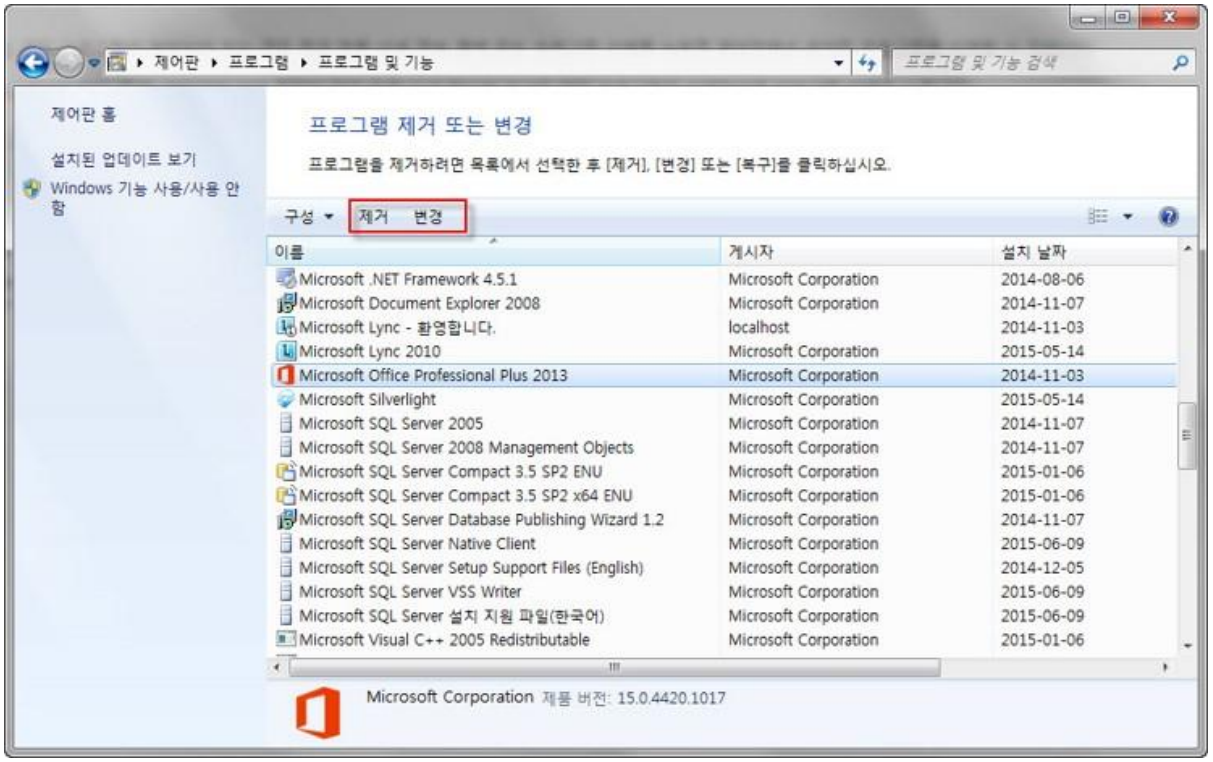
조치 방법

비인가 프로그램이 설치되어 있는 경우 프로그램 삭제를 누르면 제어판에서 설치된 프로그램을 삭제할 수 있습니다.

1. 비인가 프로그램 설치 점검의 점검 항목 상세 정보에 표시된 비인가 프로그램을 삭제하려면 **프로그램 삭제하기**를 누릅니다.



2. 제어판이 나타나면, 삭제 대상 프로그램을 선택하고 화면 상단의 **제거**나 **변경**을 눌러 해당 프로그램을 PC에서 삭제합니다.


제어판 ▸ 프로그램 ▸ 프로그램 및 기능
프로그램 및 기능 검색
제어판 홈
설치된 업데이트 보기
Windows 기능 사용/사용 안 함
프로그램 제거 또는 변경
프로그램을 제거하려면 목록에서 선택한 후 [제거], [변경] 또는 [복구]를 클릭하십시오.
구성
제거
변경
이름
게시자
설치 날짜
Microsoft .NET Framework 4.5.1 Microsoft Corporation 2014-08-06
Microsoft Document Explorer 2008 Microsoft Corporation 2014-11-07
Microsoft Lync - 환영합니다. localhost 2014-11-03
Microsoft Lync 2010 Microsoft Corporation 2015-05-14
Microsoft Office Professional Plus 2013 Microsoft Corporation 2014-11-03
Microsoft Silverlight Microsoft Corporation 2015-05-14
Microsoft SQL Server 2005 Microsoft Corporation 2014-11-07
Microsoft SQL Server 2008 Management Objects Microsoft Corporation 2014-11-07
Microsoft SQL Server Compact 3.5 SP2 ENU Microsoft Corporation 2015-01-06
Microsoft SQL Server Compact 3.5 SP2 x64 ENU Microsoft Corporation 2015-01-06
Microsoft SQL Server Database Publishing Wizard 1.2 Microsoft Corporation 2014-11-07
Microsoft SQL Server Native Client Microsoft Corporation 2015-06-09
Microsoft SQL Server Setup Support Files (English) Microsoft Corporation 2014-12-05
Microsoft SQL Server VSS Writer Microsoft Corporation 2015-06-09
Microsoft SQL Server 설치 지원 파일(한국어) Microsoft Corporation 2015-06-09
Microsoft Visual C++ 2005 Redistributable Microsoft Corporation 2015-01-06
Microsoft Corporation 제품 버전: 15.0.4420.1017

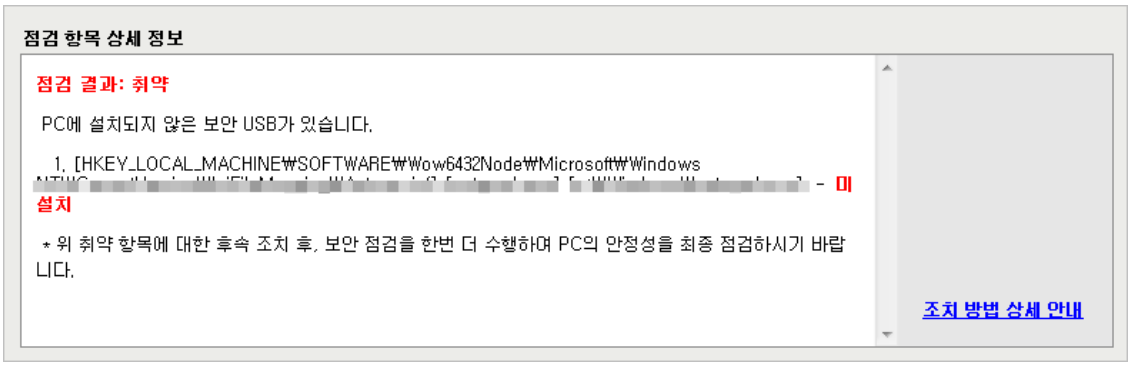
보안 USB 설치 점검

관리자가 지정한 보안 USB 가 설치되어 있는지를 점검하고, 미 설치 시에는 담당자에게 문의하여 보안 USB 제품을 설치해야 합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: 관리자가 지정한 보안 USB 가 설치되어 있습니다.
- 취약: 관리자가 지정한 보안 USB 가 설치되어 있지 않습니다.



조치 방법

관리자가 지정한 보안 USB 가 설치되어 있지 않은 경우에는 담당자에게 문의하여 보안 USB 제품을 설치하시기 바랍니다.

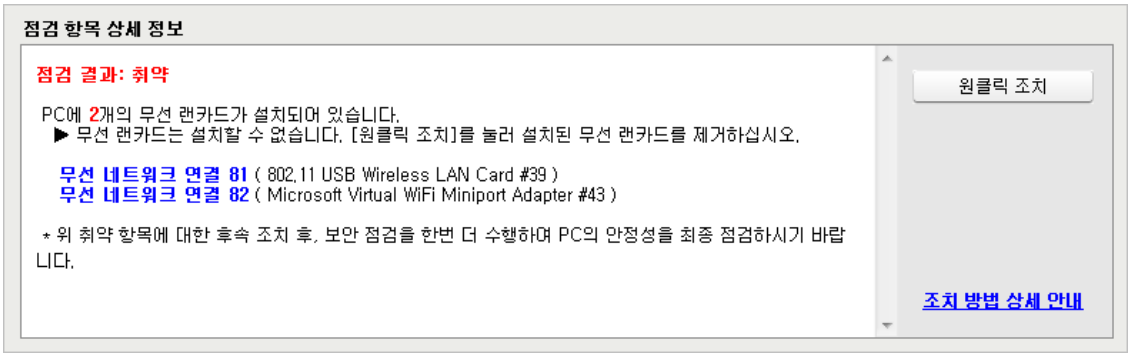
무선 랜카드 설치 점검

무선 랜카드 설치가 되어있는지 확인하여 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: 무선 랜카드가 설치되어 있지 않습니다.
- 취약: 무선 랜카드가 설치되어 있습니다. **원클릭 조치**를 눌러 설치된 무선 랜카드를 제거하십시오.



참고

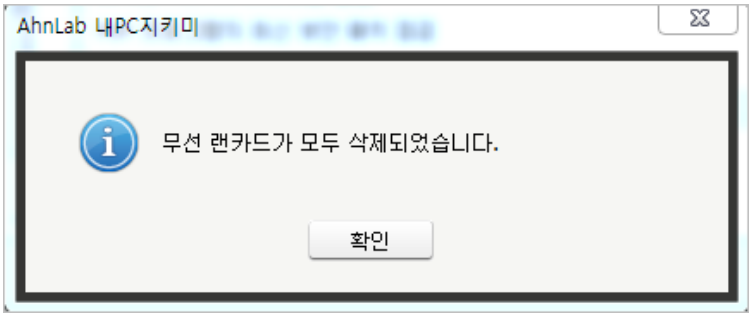
노트북에 무선 랜카드가 설치되어 있는 경우 점검 결과가 항상 취약으로 표시됩니다.

조치 방법

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. 무선 랜카드를 삭제하면 다음과 같은 알림 창이 나타납니다.



3. 알림 창에서 **확인**을 누릅니다. 점검 결과는 안전으로 변경됩니다.

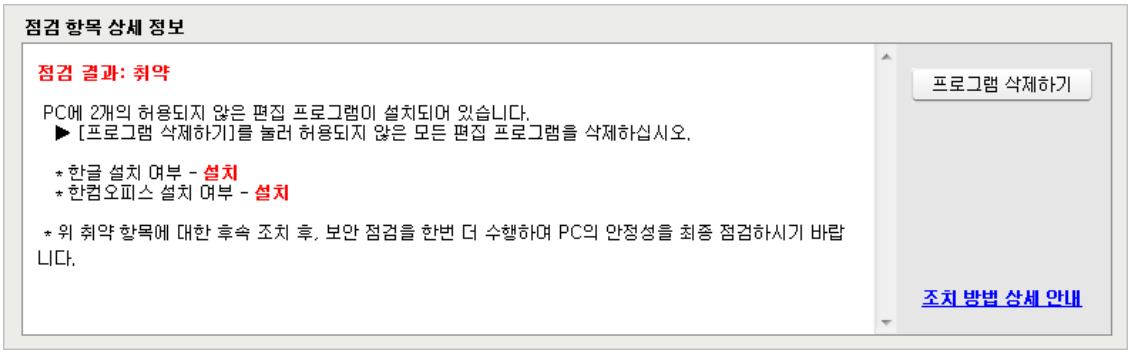
편집 프로그램 설치 점검

라이선스가 없는 편집 프로그램 설치 여부를 확인하기 위해 MS 워드, 한글, PDF 등 관리자가 점검 대상으로 설정한 편집 프로그램이 PC 에 설치되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

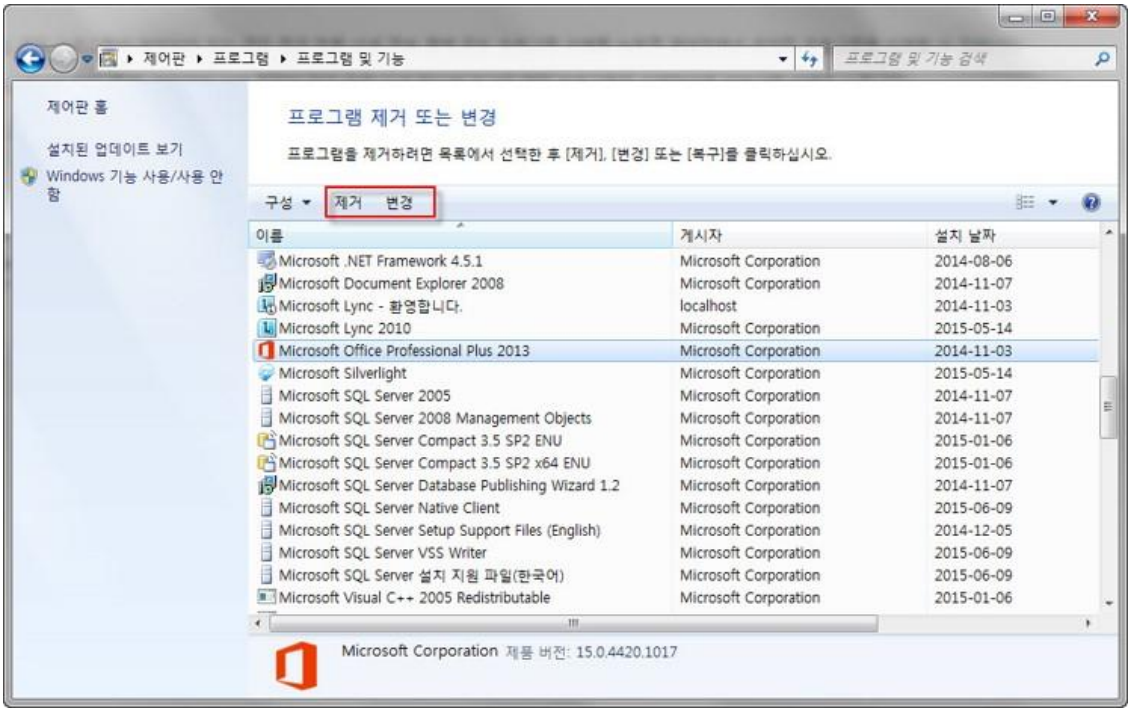
- 안전: PC 에 허용된 편집 프로그램만 설치되어 있습니다.
- 취약: 점검 결과가 취약으로 나오는 경우, 관리자가 지정한 편집 프로그램이 설치되어 있는 경우, 설치 정보가 나타납니다.



조치 방법

라이선스가 없는 편집 프로그램이 설치되어 있는 경우 점검 항목 상세 정보에서 **프로그램 삭제**를 누르면 제어판에서 설치된 프로그램을 삭제할 수 있습니다.

1. 편집 프로그램(MS 워드, 한글, PDF)설치 점검의 점검 결과로 나타난 항목을 삭제하려면 **프로그램 삭제**를 누릅니다.
2. 제어판이 나타나면, 삭제 대상 프로그램을 선택하고 화면 상단의 **제거**를 누르면 해당 프로그램을 PC 에서 삭제합니다.



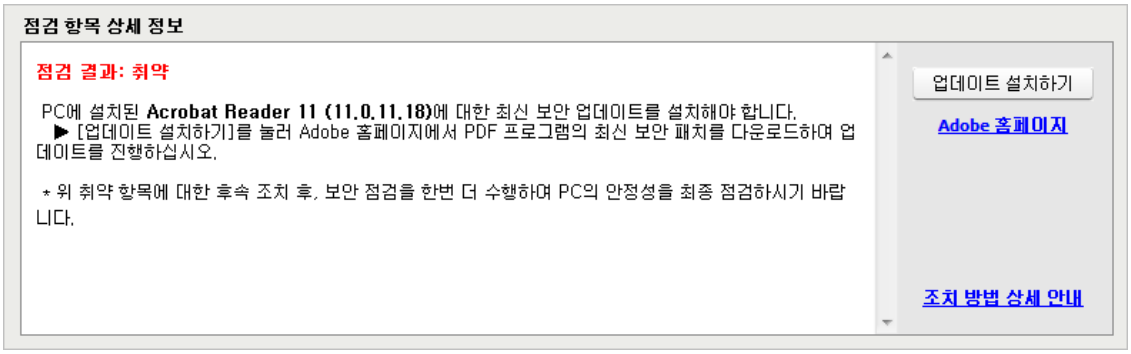
PDF 프로그램의 최신 보안 패치 점검

Adobe PDF 프로그램이 최신 보안 패치를 설치했는지 여부를 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 의 PDF 프로그램이 최신 보안 패치가 적용된 최신 상태입니다.
- 취약: 점검 결과가 취약으로 나오는 경우, PDF 프로그램의 최신 버전 정보가 나타납니다. **[업데이트 설치하기]**를 눌러 Adobe 홈페이지에서 PDF 프로그램의 최신 보안 패치를 다운로드 하여 업데이트를 진행하십시오.



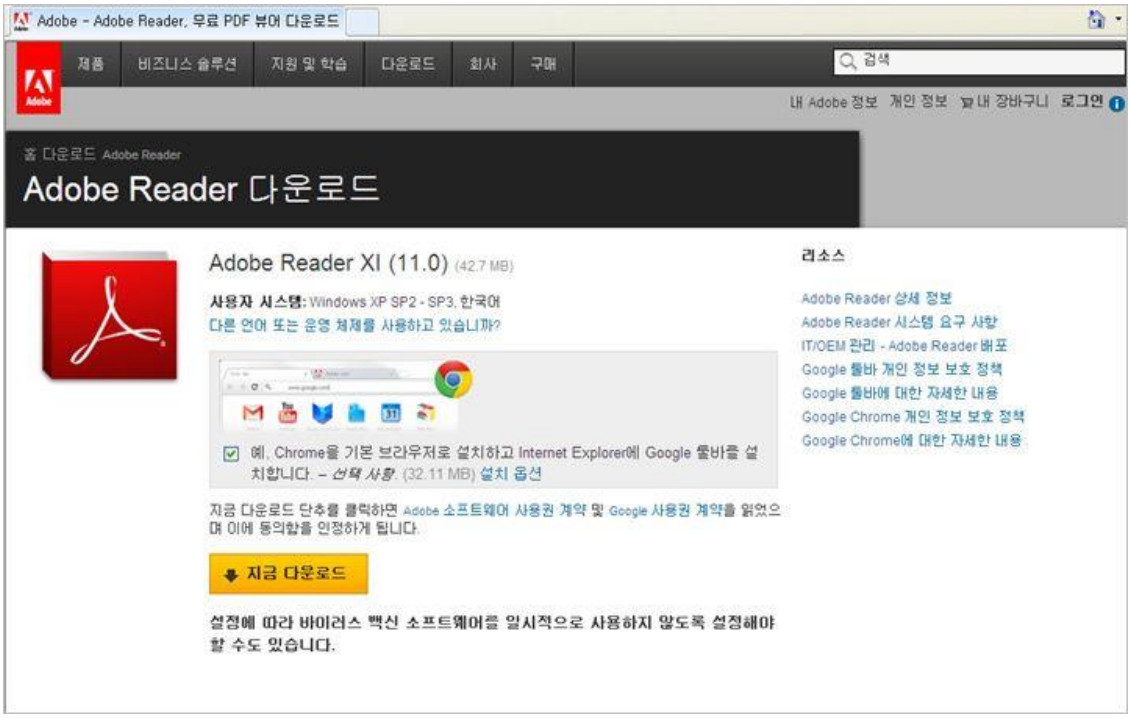
조치 방법

점검 결과가 **취약**일 때, APM 라이선스가 없는 경우와 APM 라이선스가 있는 경우에 따라 다음과 같이 조치하여 주시기 바랍니다.

[APM 라이선스가 없는 경우]

PDF 프로그램의 최신 보안 패치를 적용하려면 다음과 같은 방법으로 조치할 수 있습니다.

- 점검 항목 상세 정보에서 **업데이트 설치하기**를 눌러 Adobe PDF 프로그램의 최신 보안 패치를 적용합니다.
- Adobe 홈페이지에 접속하여 최신 버전의 업데이트 파일을 다운로드 하여 설치합니다.



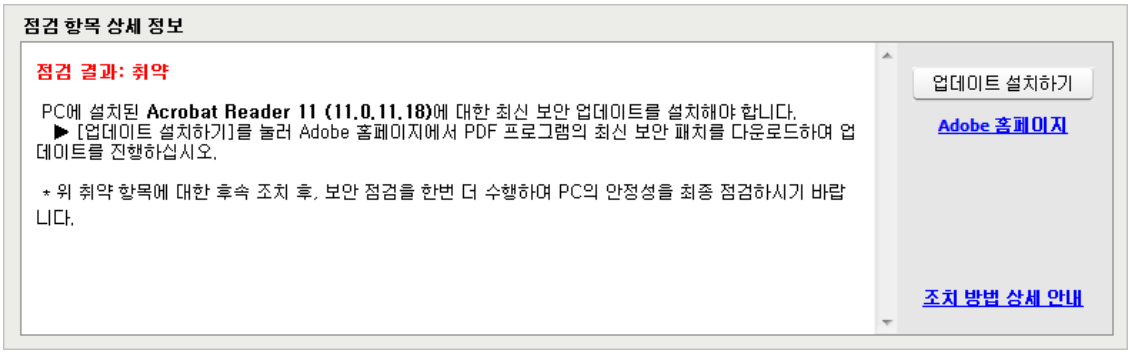
참고

다운로드 웹 페이지의 주소(http://get.adobe.com/kr/reader)는 변경될 수 있으므로 해당 내용은 Adobe 사 홈페이지에서 확인해야 합니다.

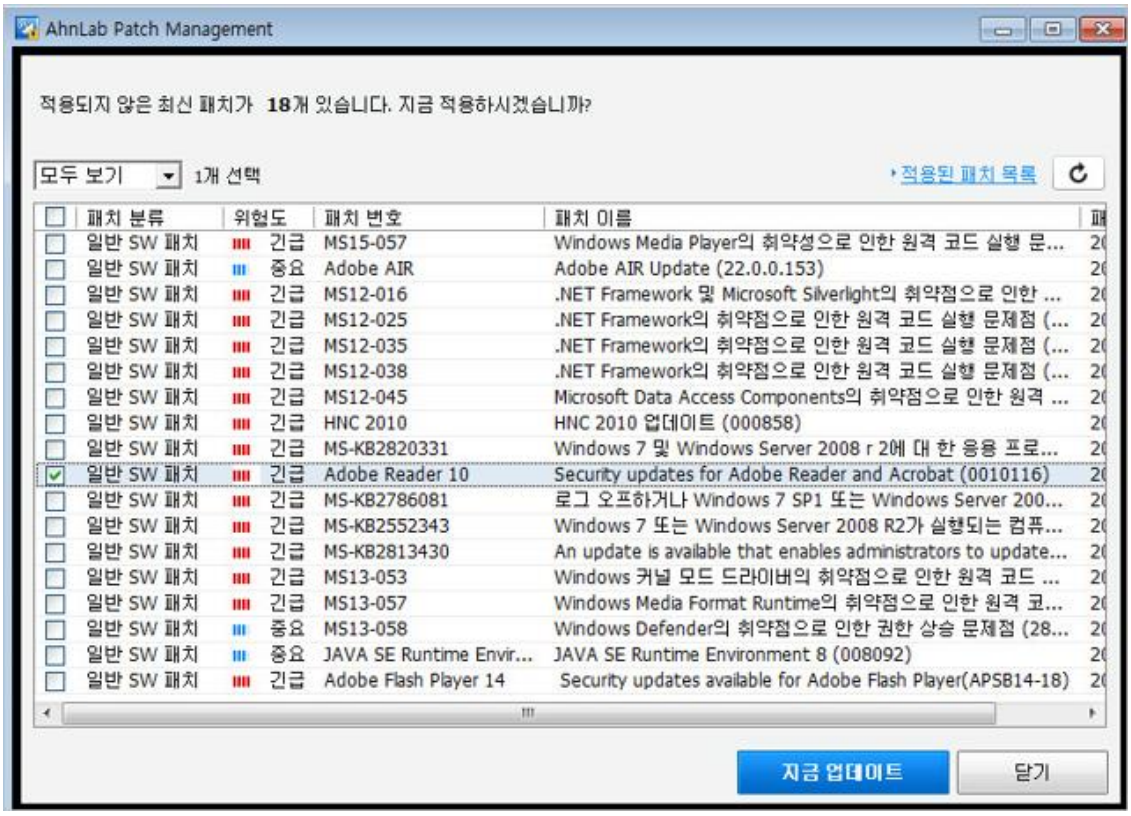
[APM 라이선스가 있는 경우]

APM 제품을 통해 적용되지 않은 패치 목록을 확인하고 최신 보안 패치를 적용할 수 있습니다.

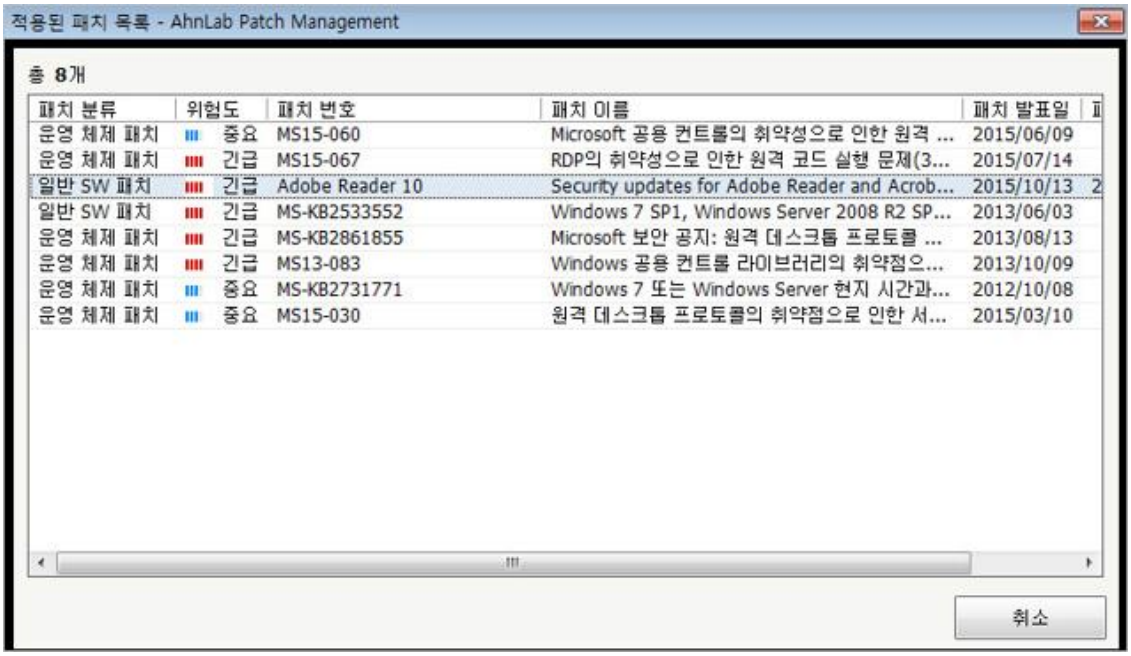
1. 업데이트 설치하기를 누릅니다.



2. APM이 실행되며 <패치 정보 보기>에서 현재 사용자 PC에 적용되지 않은 패치 목록을 확인할 수 있습니다.



3. **지금 업데이트**를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.
4. 패치 적용이 완료되면 화면 상단의 **적용된 패치 목록**을 눌러 설치된 패치 정보를 확인할 수 있습니다.



확장 취약점 점검 목록

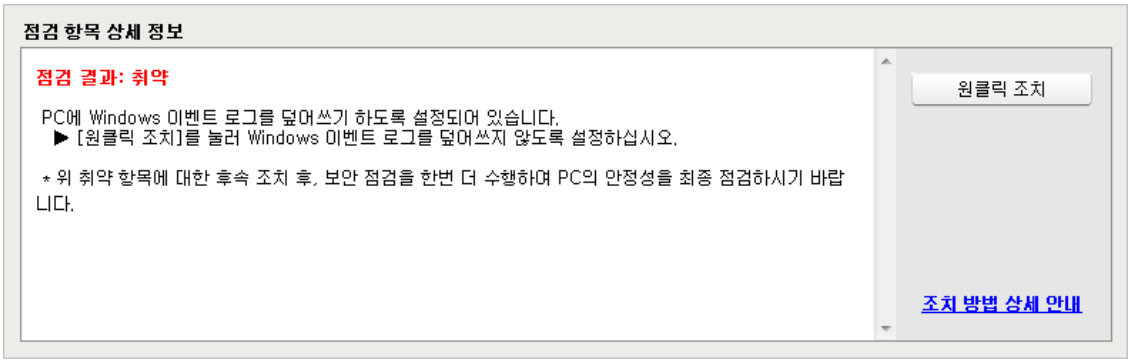
Windows 이벤트 로그 덮어쓰기 설정 점검

사용자 PC 에 Windows 이벤트 로그가 덮어쓰기 하도록 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 의 Windows 이벤트 로그가 덮어쓰기 하지 않도록 설정되어 있습니다.
- 취약: PC 에 Windows 이벤트 로그를 덮어쓰기 하도록 설정되어 있습니다. **원클릭 조치**를 눌러 Windows 이벤트 로그를 덮어쓰지 않도록 설정하십시오.

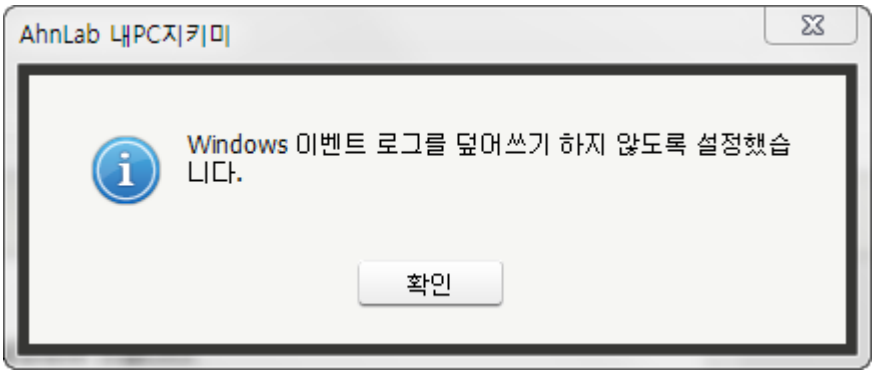


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

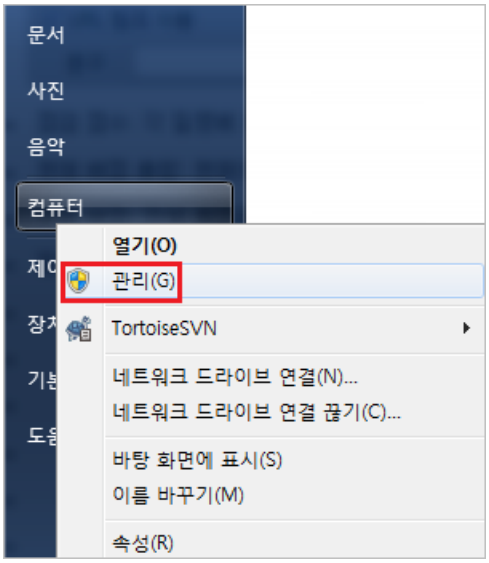
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. Windows 이벤트 로그를 덮어쓰기 하지 않도록 설정이 변경되면 다음과 같은 알림 창이 나타납니다.



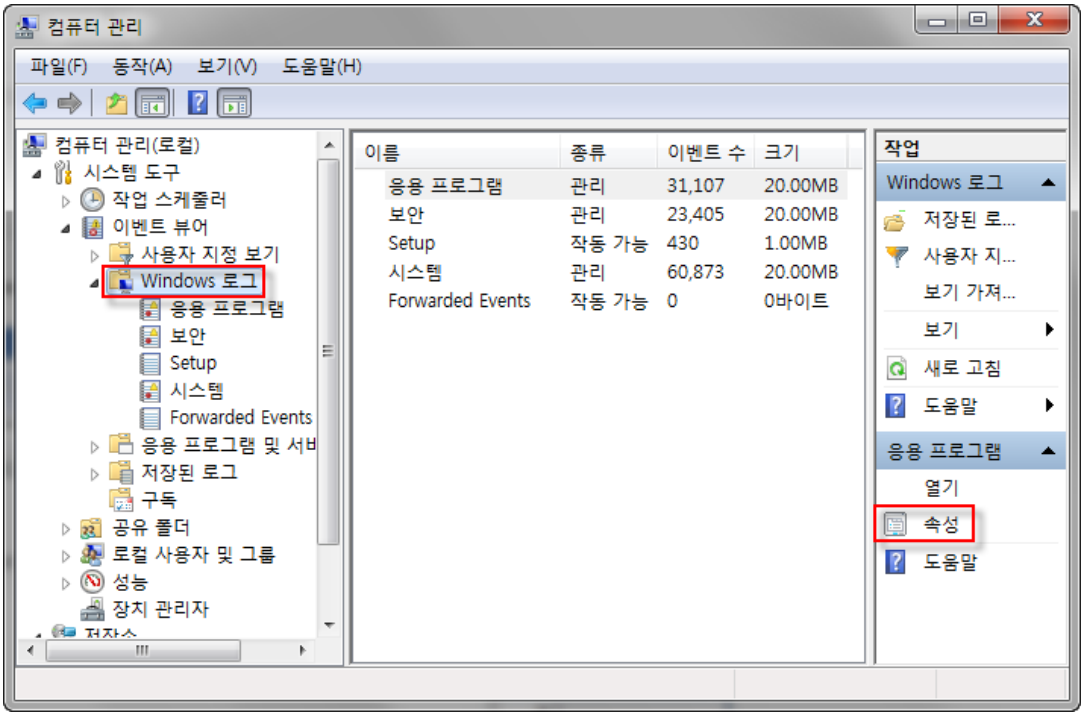
3. 알림 창에서 **확인**을 누릅니다. 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. 작업 표시줄의 **시작** > **컴퓨터**에서 마우스 오른쪽 버튼을 클릭하여 **관리**를 선택합니다.

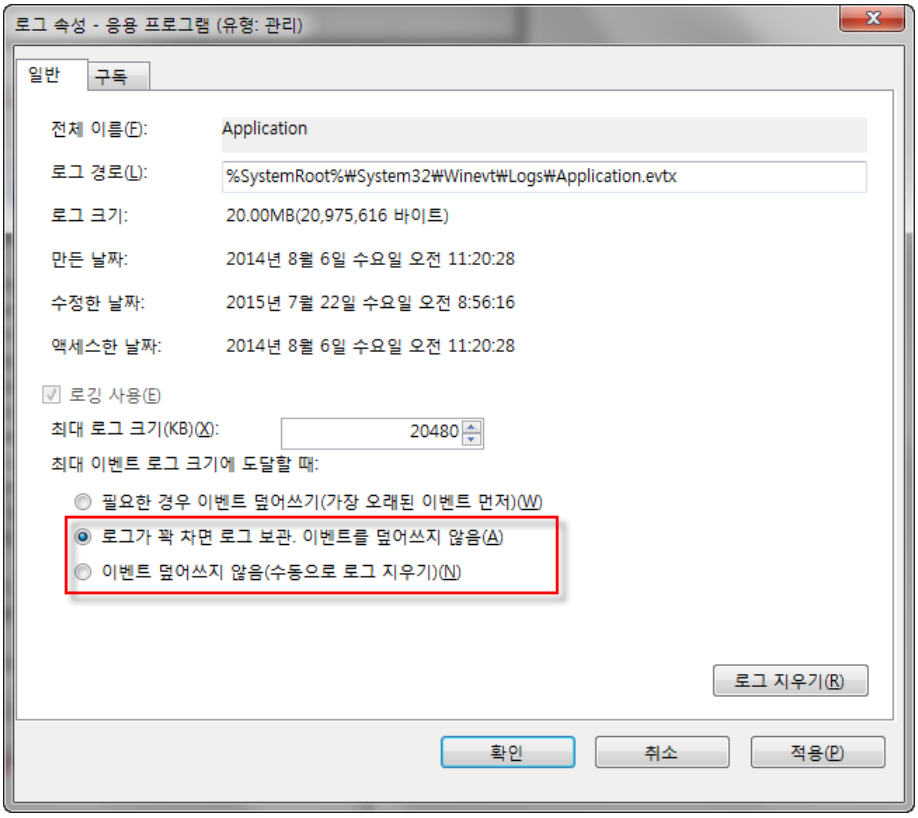


2. 컴퓨터 관리 > 이벤트 뷰어 > Windows 로그에서 다음과 같이 오른쪽 작업 탭에서 속성을 클릭합니다.



3. <로그 속성>에서 **최대 이벤트 로그 크기에 도달할 때**의 옵션을 다음 2가지 중 1가지로 선택해야 합니다.

- 로그가 꽉 차면 로그 보관. 이벤트를 덮어쓰지 않음
- 이벤트 덮어쓰지 않음(수동으로 로그 지우기)



참고

로그 속성에서 최대 이벤트 로그 크기에 도달할 때, **필요한 경우 이벤트 덮어쓰기(가장 오래된 이벤트 먼저)** 항목으로 설정되어 있는 경우, 설정을 해제하십시오.

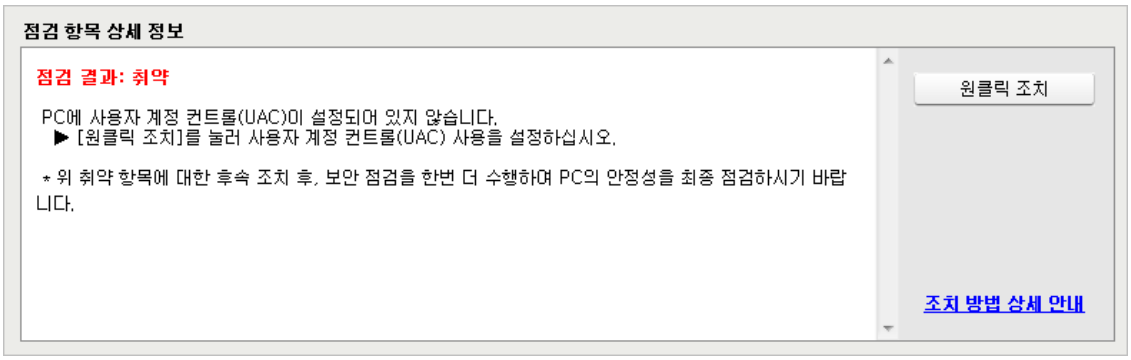
사용자 계정 컨트롤(UAC) 설정 점검

사용자 계정 컨트롤(UAC)를 사용하도록 설정되어 있는지 여부를 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 사용자 계정 컨트롤(UAC)이 설정되어 있습니다.
- 취약: PC 에 사용자 계정 컨트롤(UAC)이 설정되어 있지 않습니다. **원클릭 조치**를 눌러 사용자 계정 컨트롤(UAC) 사용을 설정하십시오.

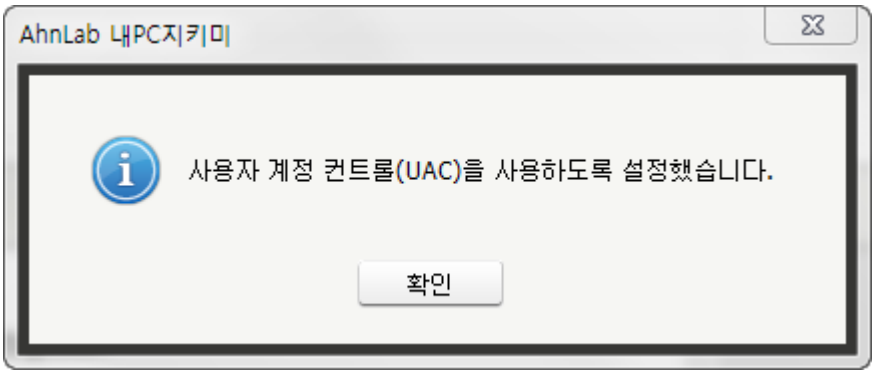


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. UAC를 사용하도록 설정이 변경되면 다음과 같은 알림 창이 나타납니다.

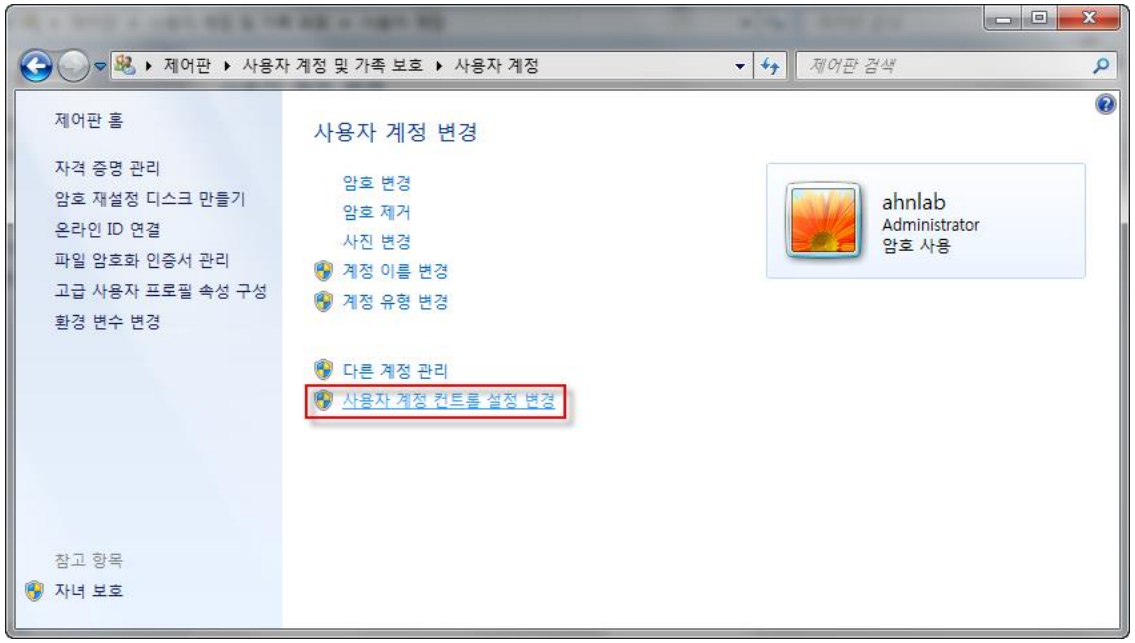


3. 알림 창에서 **확인**을 누릅니다. 점검 결과는 안전으로 변경됩니다.

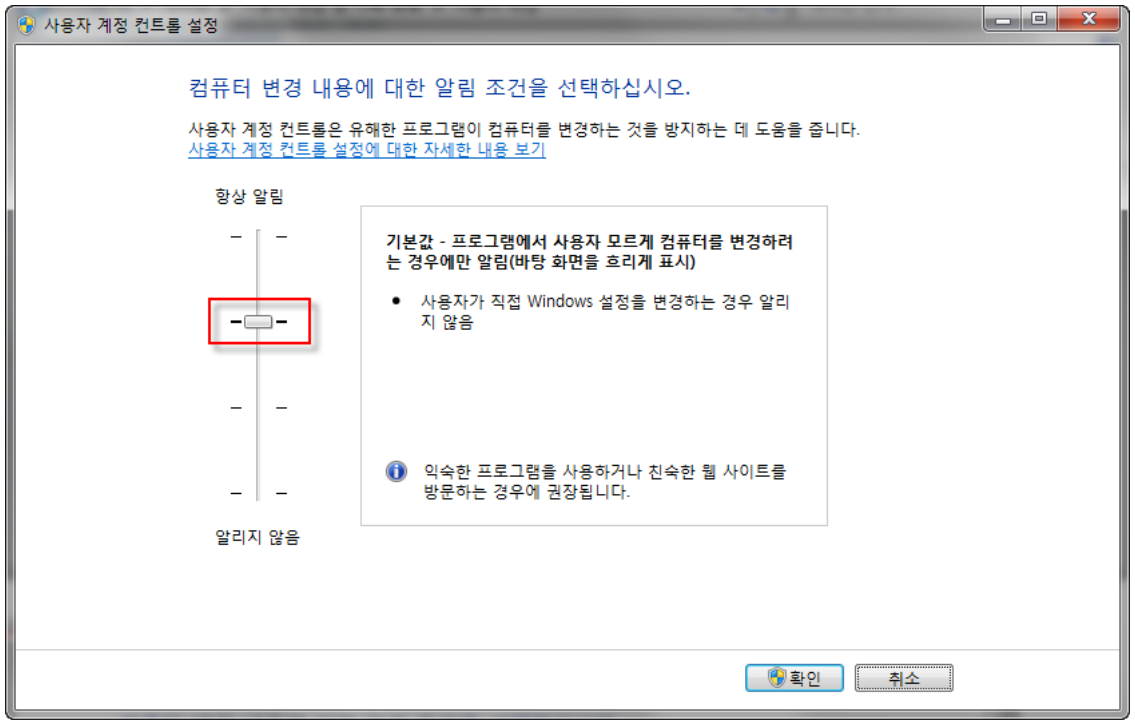
[사용자 조치]

제어판의 사용자 계정에서도 UAC 를 사용하도록 설정을 변경할 수 있습니다.

1. Windows 작업 표시줄의 **시작** > **설정** > **제어판** > **사용자 계정 및 가족 보호** > **사용자 계정**을 선택한 후 **사용자 계정 컨트롤 설정 변경**을 선택합니다.



2. 설정 값을 권장 값으로 올려줍니다.



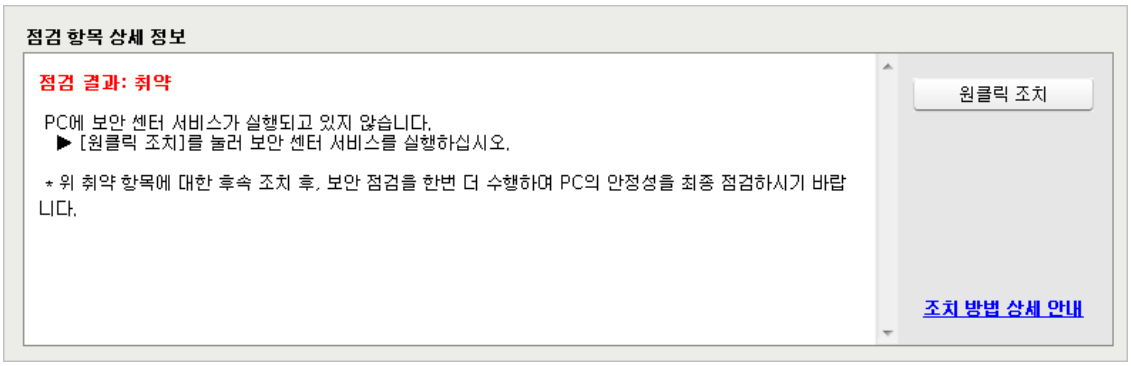
보안 센터 서비스 실행 점검

보안 센터 서비스가 실행되고 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 보안 센터 서비스가 실행되고 있습니다.
- 취약: PC 에 보안 센터 서비스가 실행되고 있지 않습니다. **원클릭 조치**를 눌러 보안 센터 서비스를 실행하십시오.



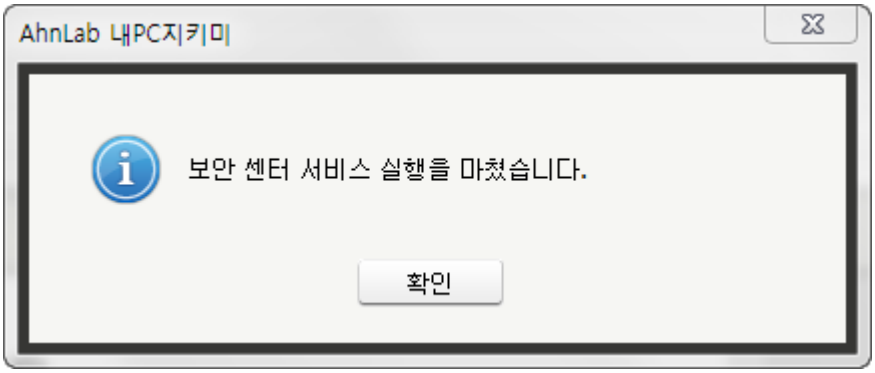
조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

점검 결과가 **취약**인 경우 점검 항목 상세 정보에서 **원클릭 조치**를 눌러 보안 센터 서비스를 시작할 수 있습니다.

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. 보안 센터 서비스를 시작하면 다음과 같은 알림 창이 나타납니다.

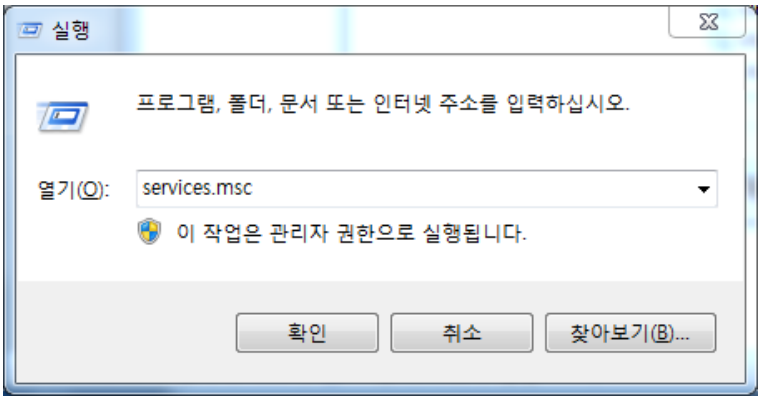


3. 알림 창에서 **확인**을 누릅니다. 점검 결과는 안전으로 변경됩니다.

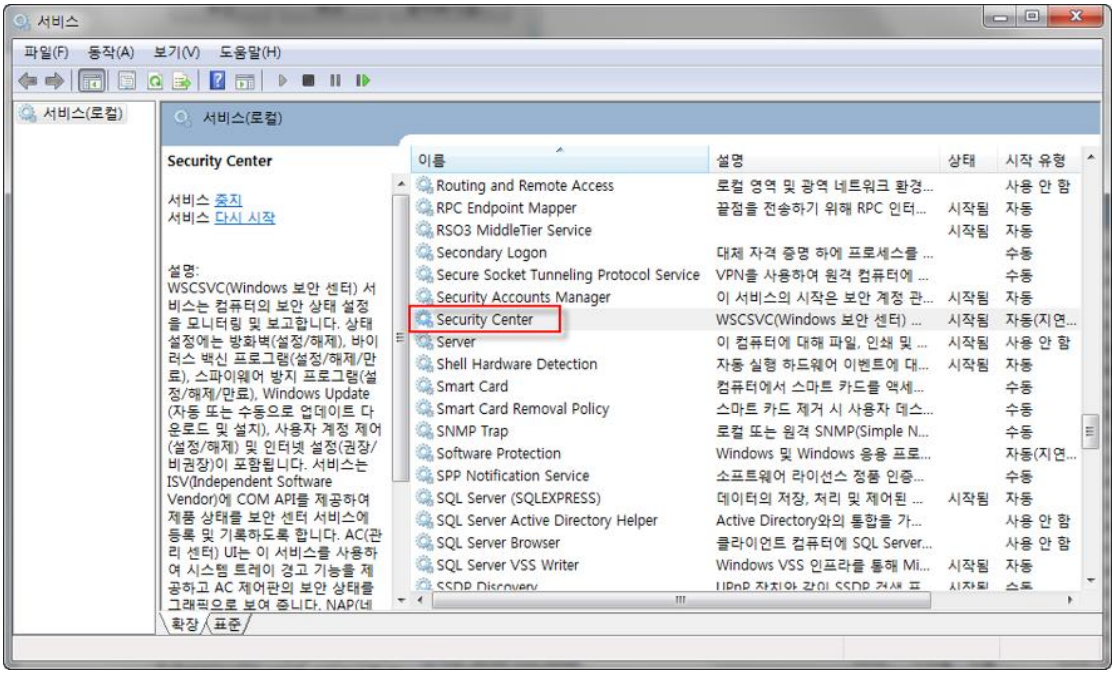
[사용자 조치]

보안 센터 서비스가 실행되고 있지 않은 경우 다음과 같은 방법으로 조치할 수 있습니다.

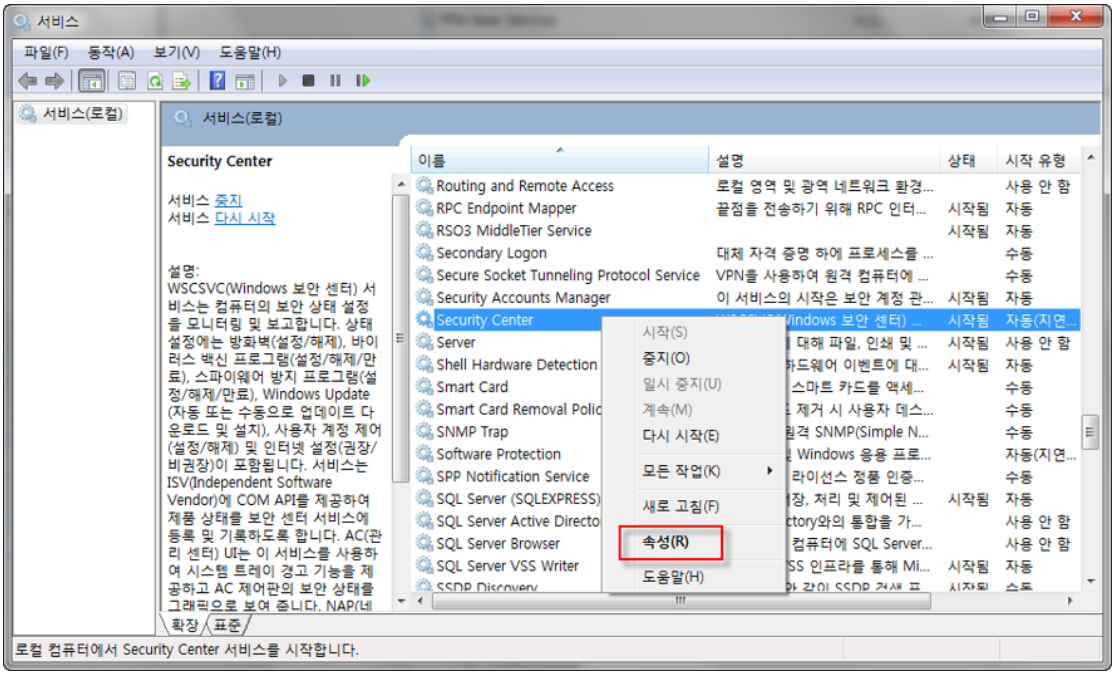
1. 윈도우 + R키를 눌러 실행 창을 띄운 후 **services.msc**를 입력합니다.



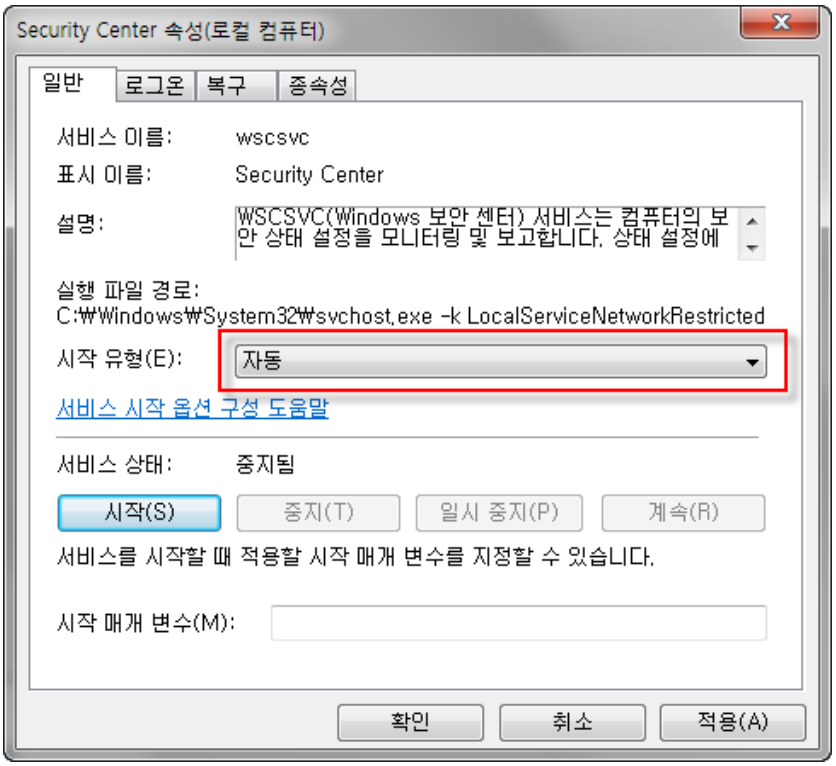
2. 서비스 목록에서 **Security Center**를 확인합니다.



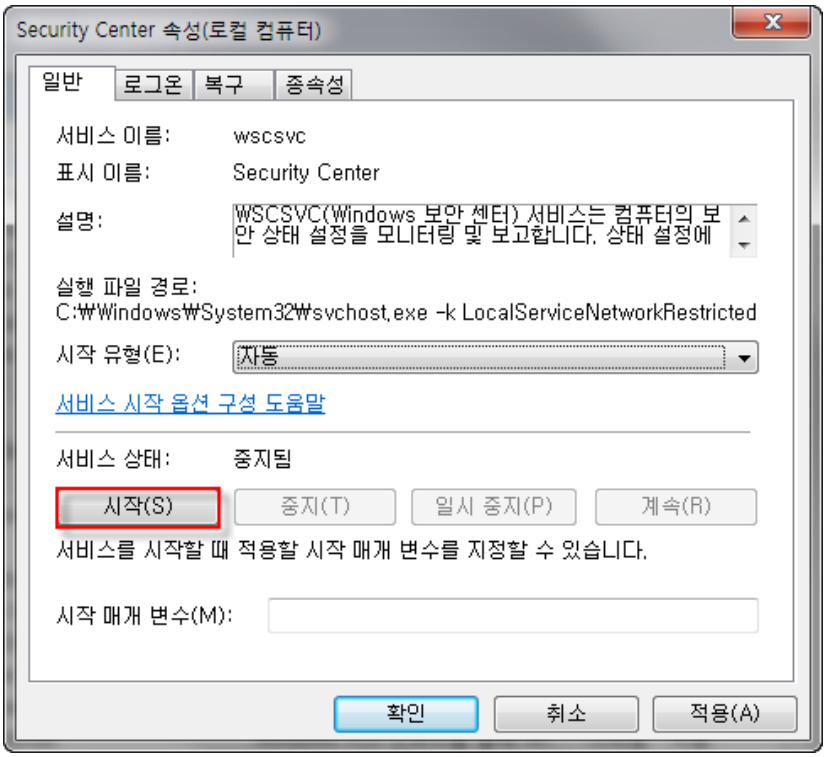
3. **Security Center** 서비스를 우클릭한 후 속성을 클릭합니다.



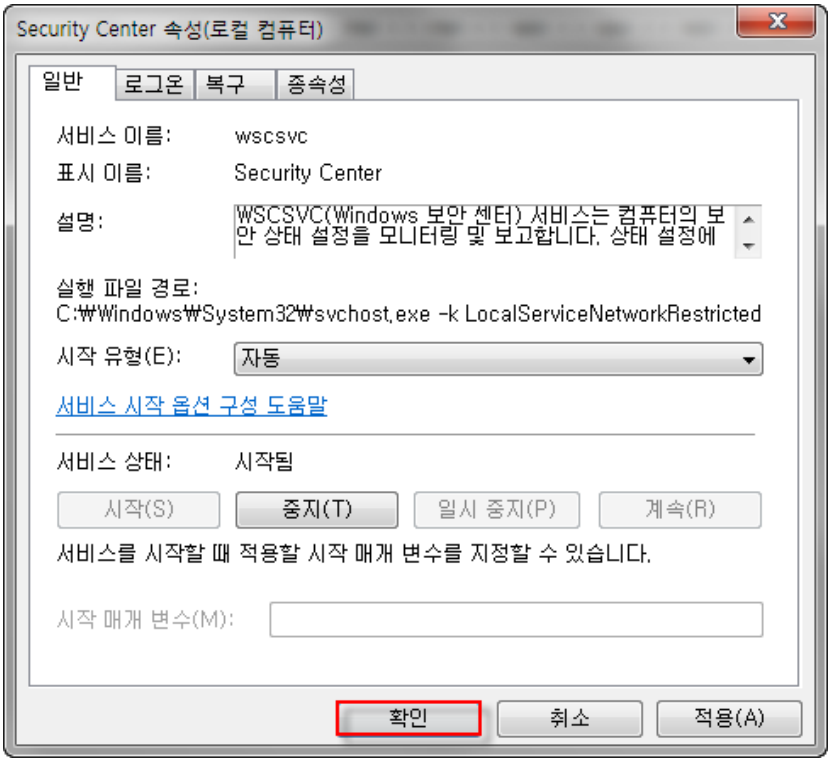
4. 시작 유형을 자동으로 설정합니다.



5. 이후 **시작**을 클릭하여 서비스를 시작합니다.



6. **확인**을 클릭하여 설정을 종료합니다.



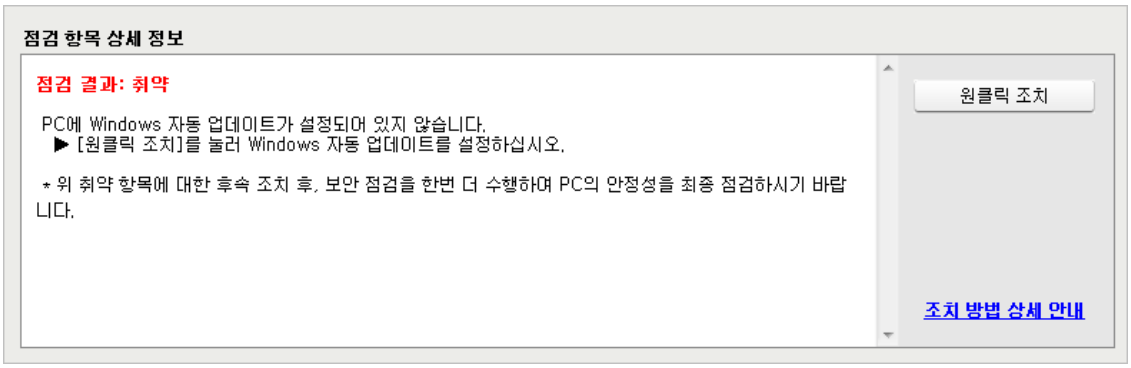
Windows 자동 업데이트 설정 점검

Microsoft 의 Windows Update 를 이용하여 자동으로 패치를 받고 업데이트하는지 여부를 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 Windows 자동 업데이트가 설정되어 있습니다.
- 취약: PC 에 Windows 자동 업데이트가 설정되어 있지 않습니다. **원클릭 조치**를 눌러 Windows 자동 업데이트를 설정하십시오.



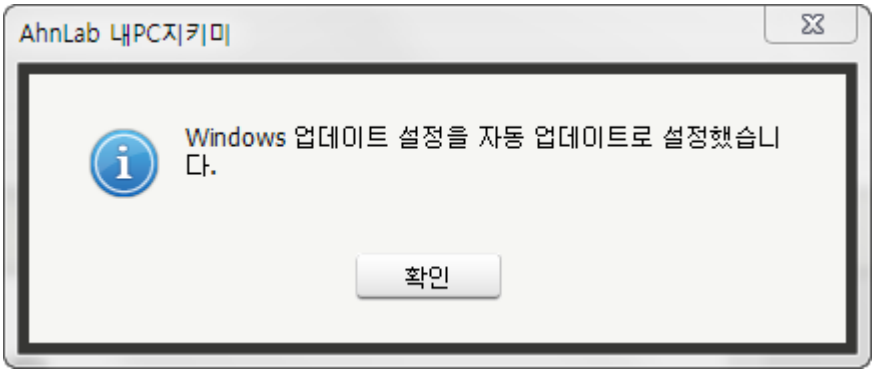
조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

1. 점검항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. 원클릭 조치로 Windows 자동 업데이트를 설정하면 다음과 같은 알림 창이 나타납니다.

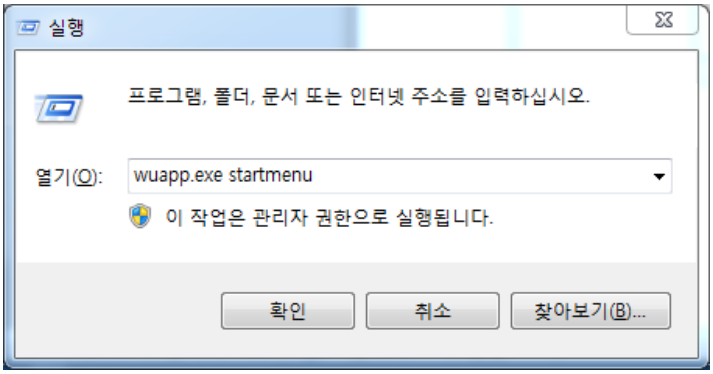


3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

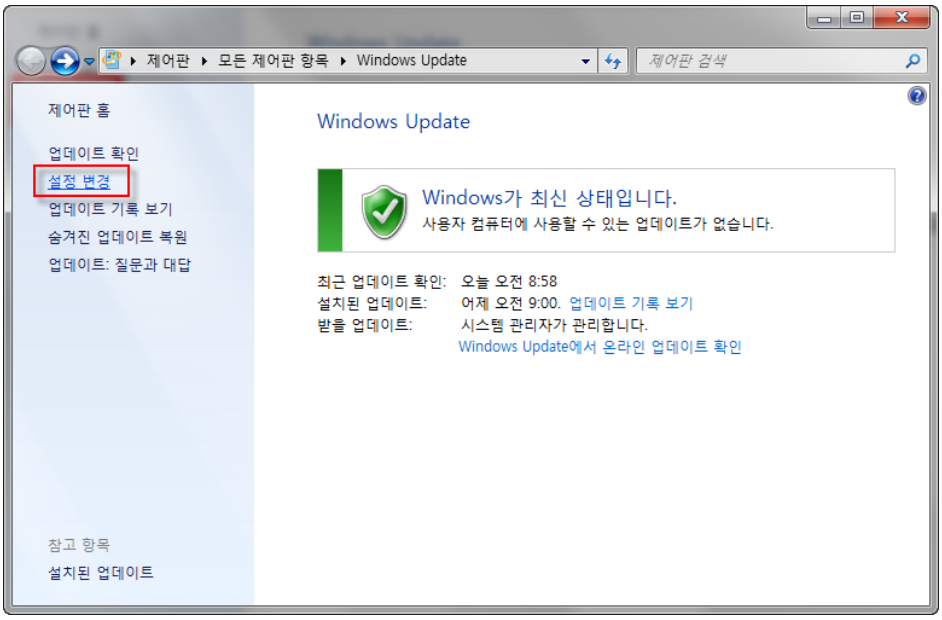
[사용자 조치]

자동 업데이트가 설정되지 않은 경우 다음과 같은 방법으로 조치할 수 있습니다.

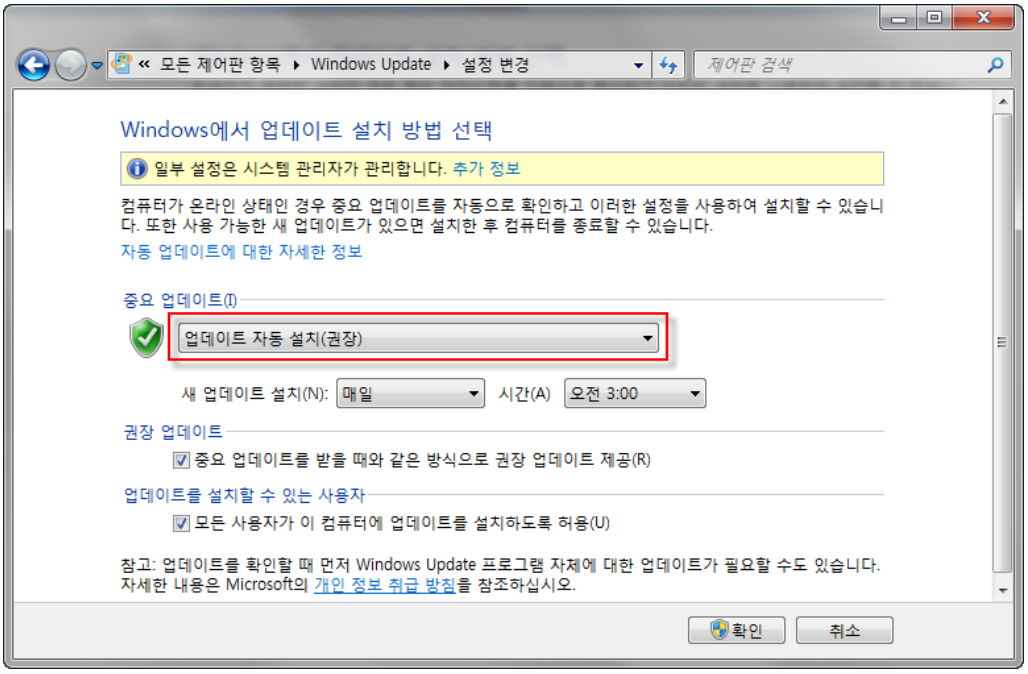
1. 윈도우 + R키를 눌러 실행 창을 띄운 후 **wuapp.exe startmenu**를 입력합니다.



2. 좌측의 설정 변경을 클릭합니다.



3. **중요 업데이트 항목을 업데이트 자동 설치(권장)**으로 설정 후 **확인**을 클릭합니다.



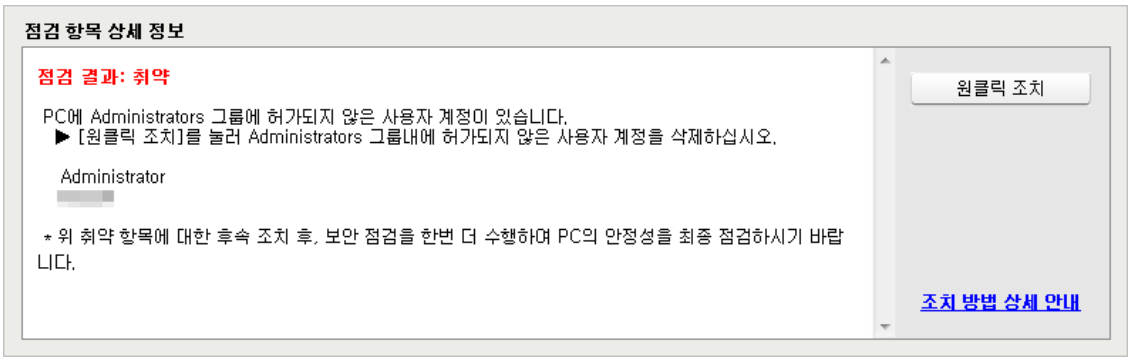
Administrators 그룹 내 사용자 계정 점검

사용자 PC 의 Administrators 그룹에 허가된 사용자만 포함되어 있는 지를 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: Administrators 그룹 내에 허가된 사용자만 있습니다.
- 취약: PC 에 Administrators 그룹에 허가되지 않은 사용자 계정이 있습니다. **원클릭 조치**를 눌러 Administrators 그룹 내에 허가되지 않은 사용자 계정을 삭제하십시오.



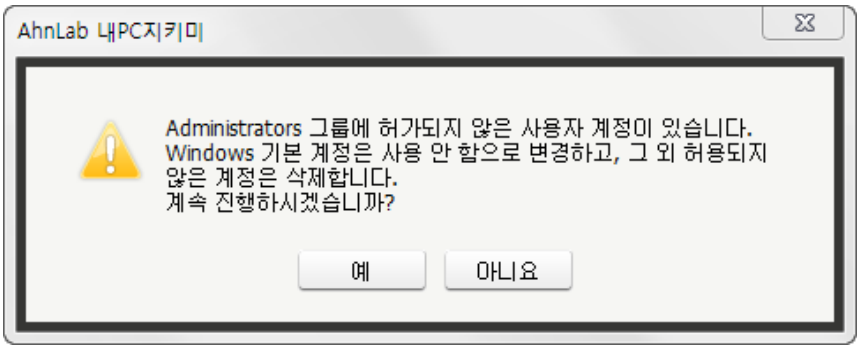
조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. 다음과 같이 Administrator 그룹에 허가되지 않은 계정을 삭제하는 경고 문구에서 **계정을 삭제하려면 예**를, **삭제하지 않으려면 아니요**를 누릅니다.



참고

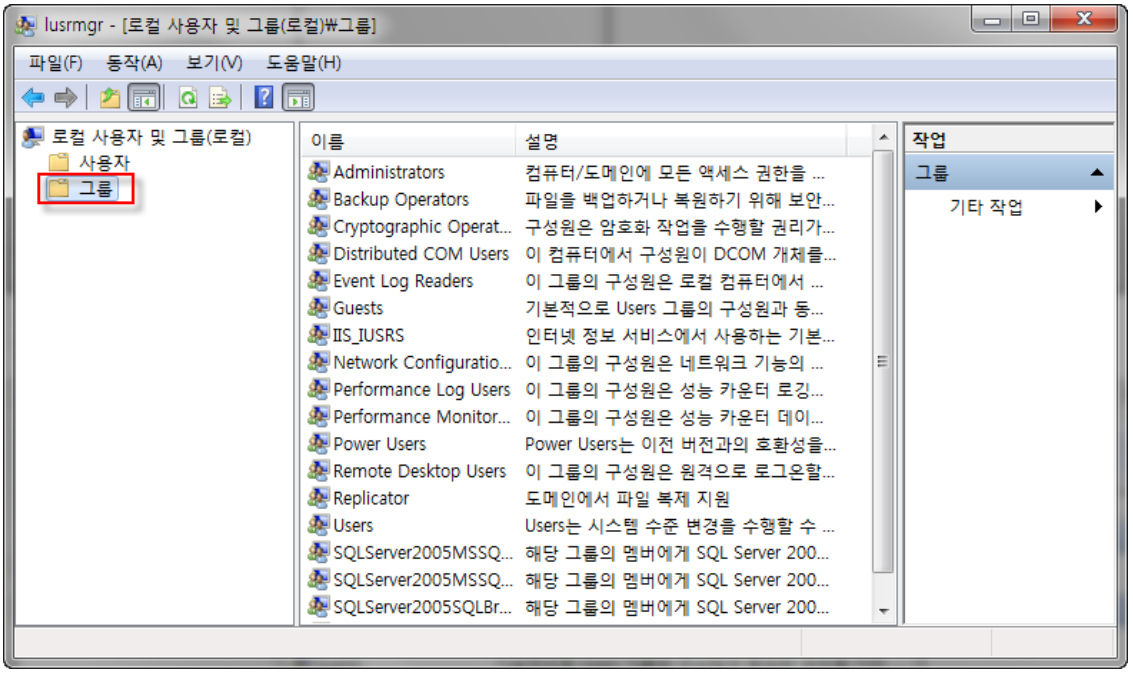
삭제한 계정은 복구할 수 없으니, 계정을 다시 한 번 확인 후 진행하십시오.

3. 알림 창에서 **예**를 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. **제어판** > **시스템 및 보안** > **관리 도구** 에서 <**컴퓨터 관리**>를 누릅니다.
2. <컴퓨터 관리>에서 로컬 사용자 및 그룹을 관리하는 설정 창이 나타납니다.

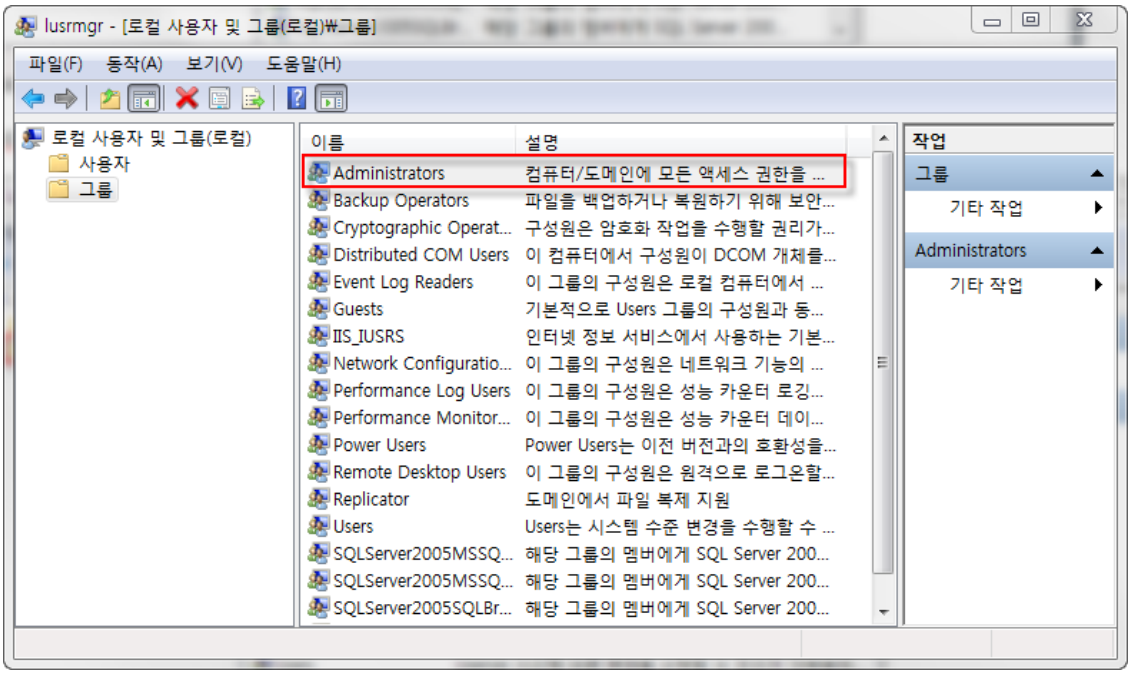
3. 실행된 <lusrmgr - [로컬 사용자 및 그룹(로컬)]>에서 왼쪽의 폴더 중에 **그룹**을 선택합니다.



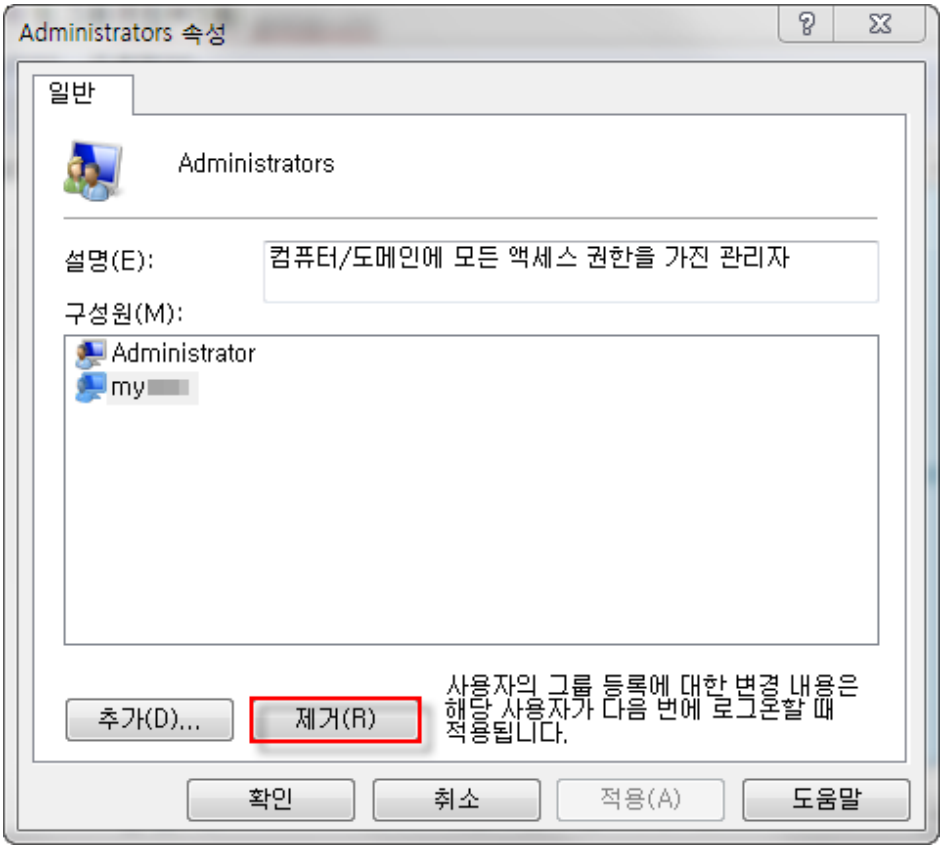
참고

<lusrmgr - [로컬 사용자 및 그룹(로컬)]>의 **그룹** 폴더는 시작 메뉴에서 **제어판** > **모든 제어판 항목** > **관리 도구** > **컴퓨터 관리**의 <컴퓨터 관리> 에서도 확인할 수 있습니다.

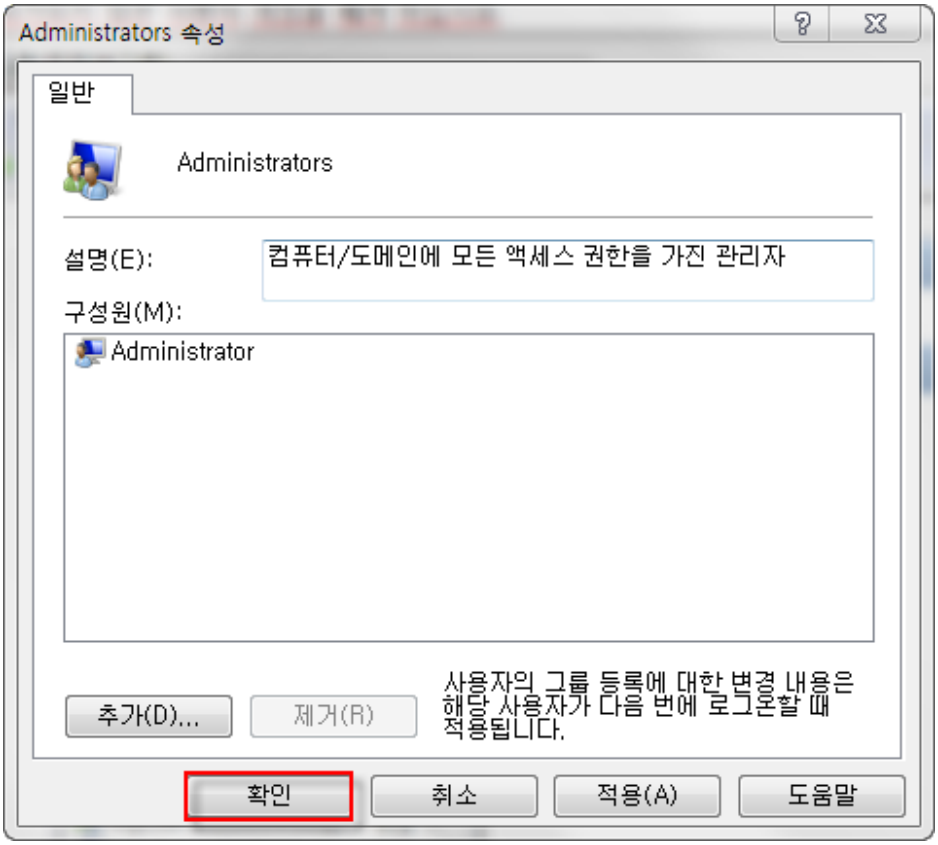
4. 그룹 폴더 내에 있는 Administrators 이름을 더블 클릭합니다.



5. <Administrators 속성>에서 허가되지 않은 사용자 계정을 **제거** 하십시오.



6. 허가되지 않은 사용자 계정을 제거한 후 **확인**을 누릅니다.



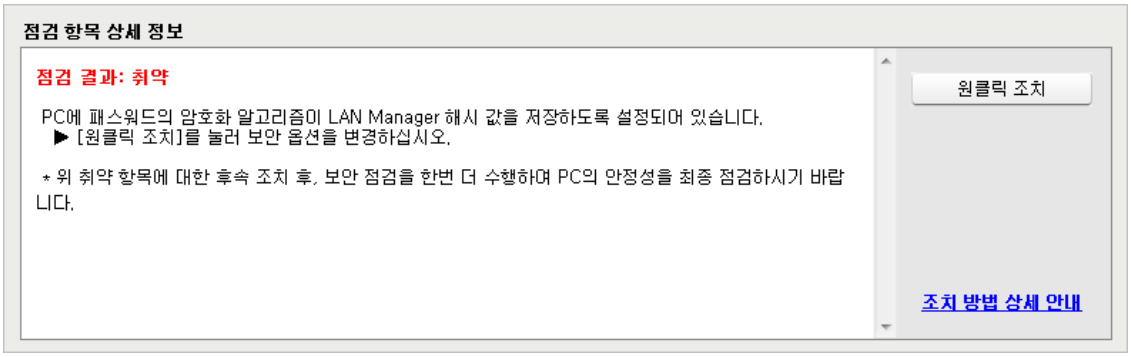
패스워드 암호화 알고리즘 설정 점검

사용자 PC 에 패스워드의 암호화 알고리즘이 LAN Manager 해시 값을 저장하도록 설정되어 있는 지 여부를 점검하여 결과를 알려줍니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 의 패스워드 보안 설정이 LAN Manager 해시 값을 저장하지 않도록 설정되어 있습니다.
- 취약: PC 의 패스워드 보안 설정이 LAN Manager 해시 값을 저장하도록 설정되어 있습니다. **원클릭 조치**를 눌러 LAN Manager 해시 값을 저장하지 않도록 보안 설정을 변경하십시오.

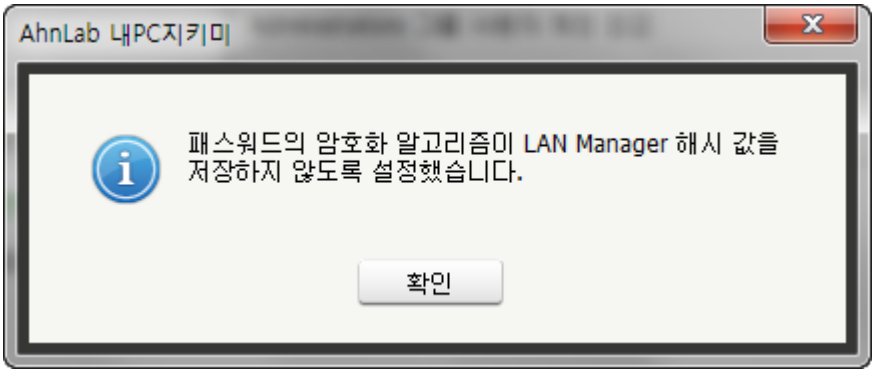


조치 방법

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. 사용자 PC에 패스워드 암호화 알고리즘이 LAN Manager 해시 값을 저장하지 않도록 설정하면 다음과 같은 알림 창이 나타납니다.



3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

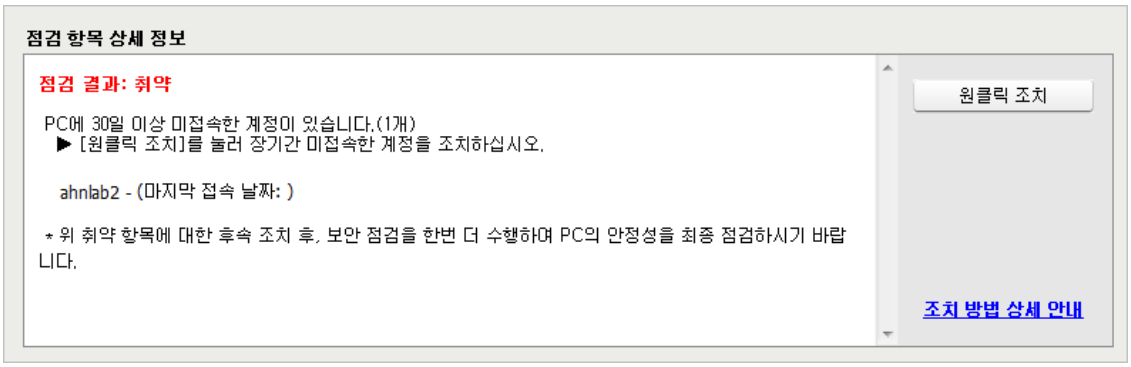
장기간 미접속 계정 점검

사용자 PC 에 장기간 동안 접속하지 않은 사용자 계정이 존재하는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 장기간 미접속한 계정이 존재하지 않습니다.
- 취약: PC 에 관리자가 설정한 기간 이상 미접속한 계정이 있습니다. **원클릭 조치**를 눌러 장기간 미접속한 계정을 조치하십시오.

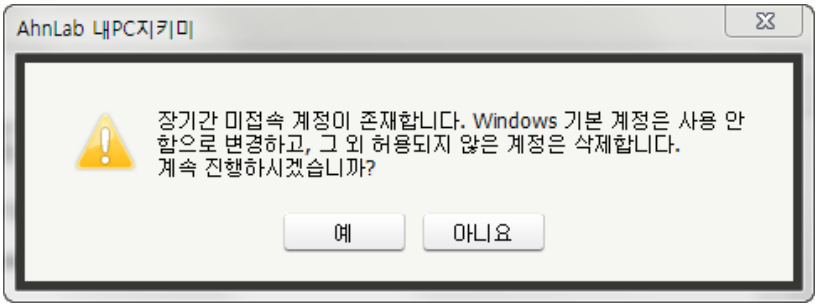


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

1. **점검 항목 상세 정보**에서 장기간 접속하지 않은 계정을 확인하고 **원클릭 조치**를 누릅니다.
2. 다음과 같이 장기간 미접속 계정에 대한 처리 방식의 선택에서 **예**를 선택하면 Windows 기본 계정은 사용 안 함으로 변경하고, 그 외 계정은 삭제합니다. **아니요**를 선택하면 설정을 변경하지 않습니다.



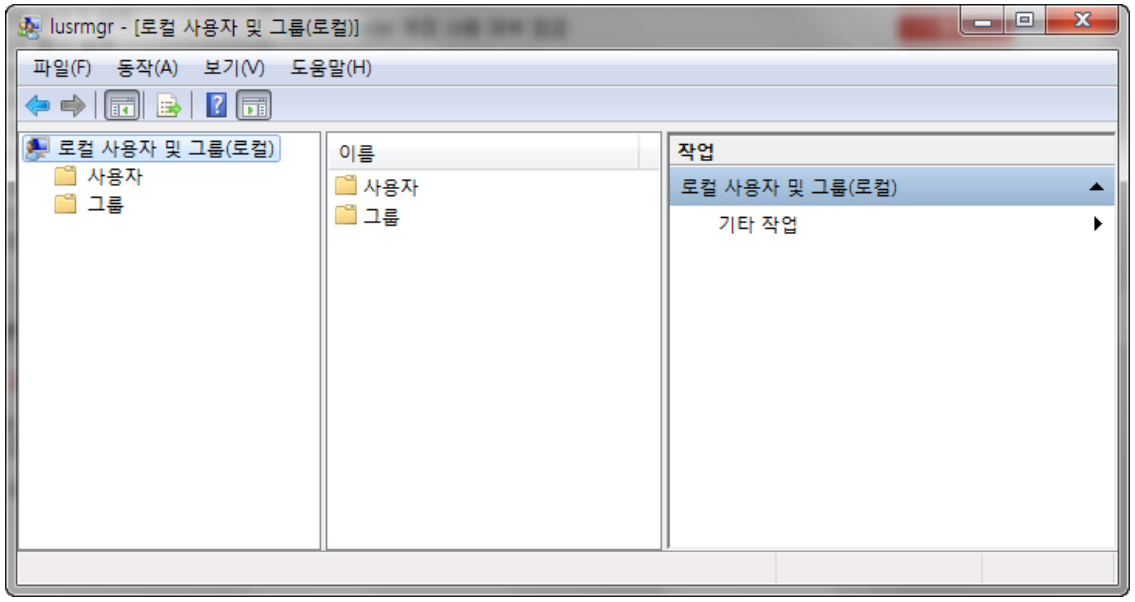
3. 알림 창에서 **예**를 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

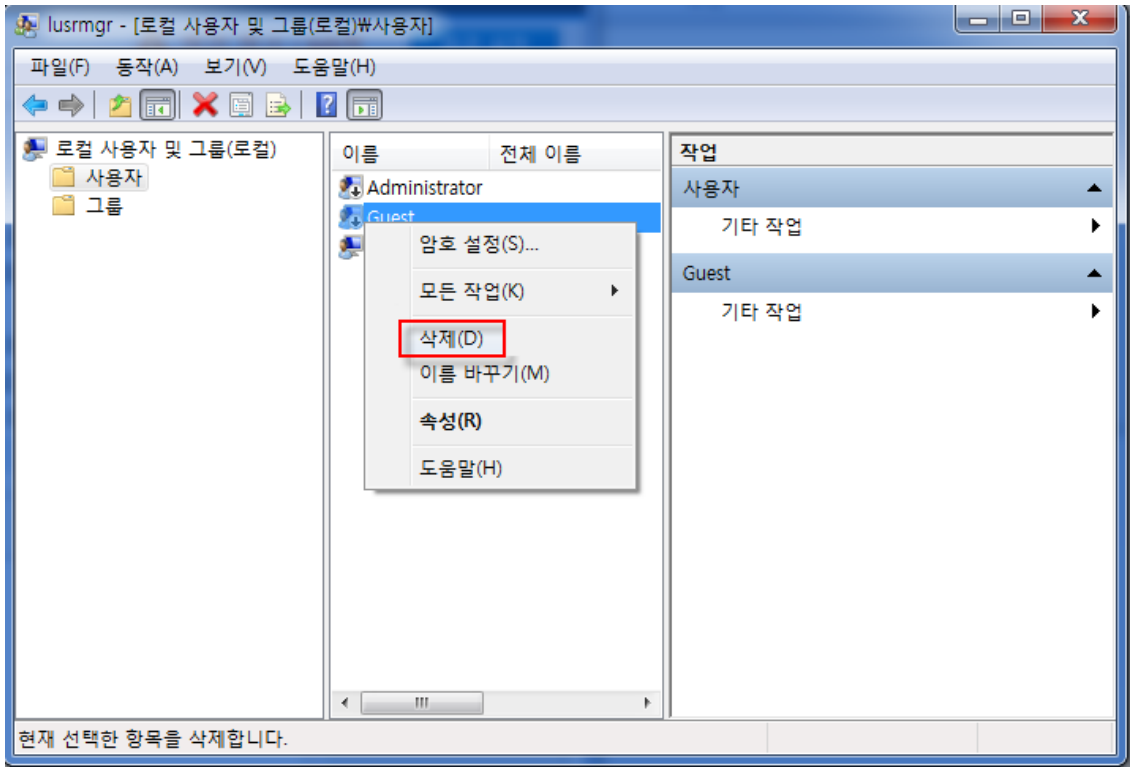
점검 결과가 **취약**인 경우, Windows Edition 의 **그룹 정책 사용 가능 여부**에 따라 각각 다른 방법으로 조치해야 합니다. Windows Edition 중 **Starter, Home, Only Core Edition** 은 그룹 정책을 사용할 수 없습니다.

그룹 정책을 사용할 수 있는 경우 (Starter, Home, Only Core 이외의 Edition)

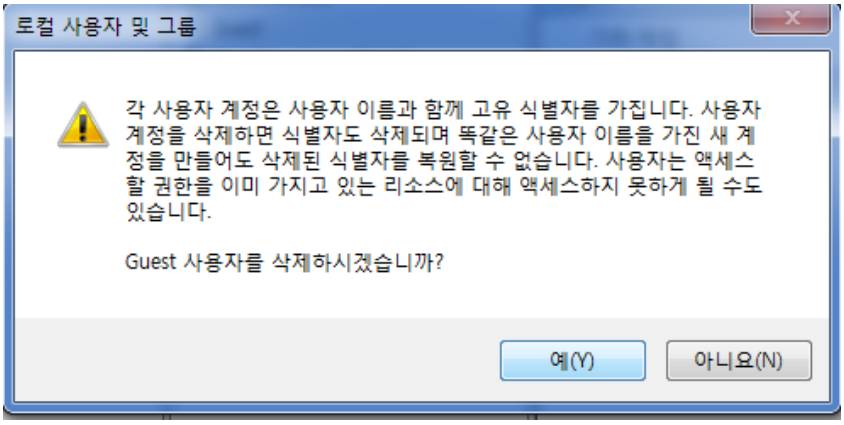
1. **제어판** > **시스템 및 보안** > **관리 도구** 에서 <**컴퓨터 관리**>를 누릅니다.
2. <컴퓨터 관리>에서 로컬 사용자 및 그룹을 관리하는 설정 창이 나타납니다.



3. **로컬 사용자 및 그룹** > **사용자**를 클릭한 후, 내 PC 지키미 에이전트에서 확인했던 장기간 미접속 계정을 선택하여 삭제를 누릅니다.



4. **예**를 클릭하면, 사용자 계정이 삭제됩니다.



그룹 정책을 사용할 수 없는 경우 (Starter, Home, Only Core Edition)

1. 시작 > 모든 프로그램 > 보조 프로그램에서 명령 프롬프트를 마우스 오른쪽 버튼으로 클릭하여, 관리자 권한으로 실행합니다.
2. <명령 프롬프트>가 실행되면 다음과 같이 명령어를 입력합니다.

   net user *계정 이름* /delete

   - **계정 이름**에는 삭제할 **장기간 미접속 계정**의 이름을 적습니다.

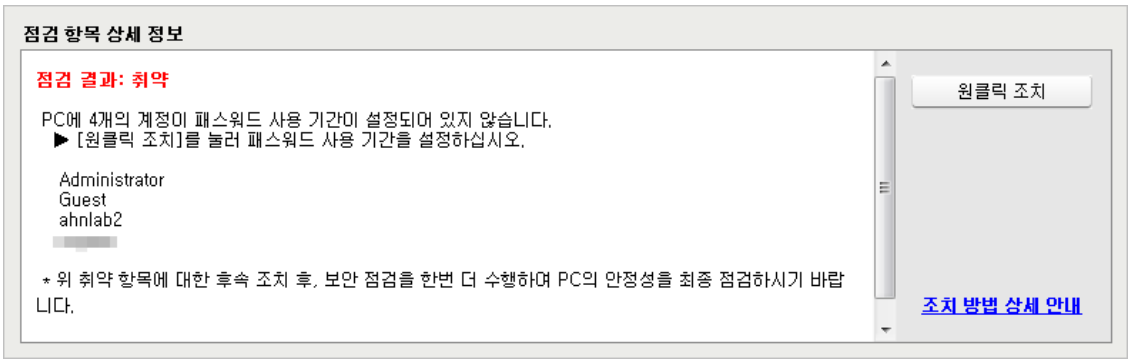
패스워드 사용 기간 제한 설정 점검

사용자 PC 에서 사용 중인 패스워드에 사용 기간 제한이 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 의 모든 계정에 패스워드 사용 기간이 설정되어 있습니다.
- 취약: PC 에 패스워드 사용 기간이 설정되지 않은 계정이 있습니다. **원클릭 조치**를 눌러 계정에 패스워드 사용 기간을 설정하십시오.



조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

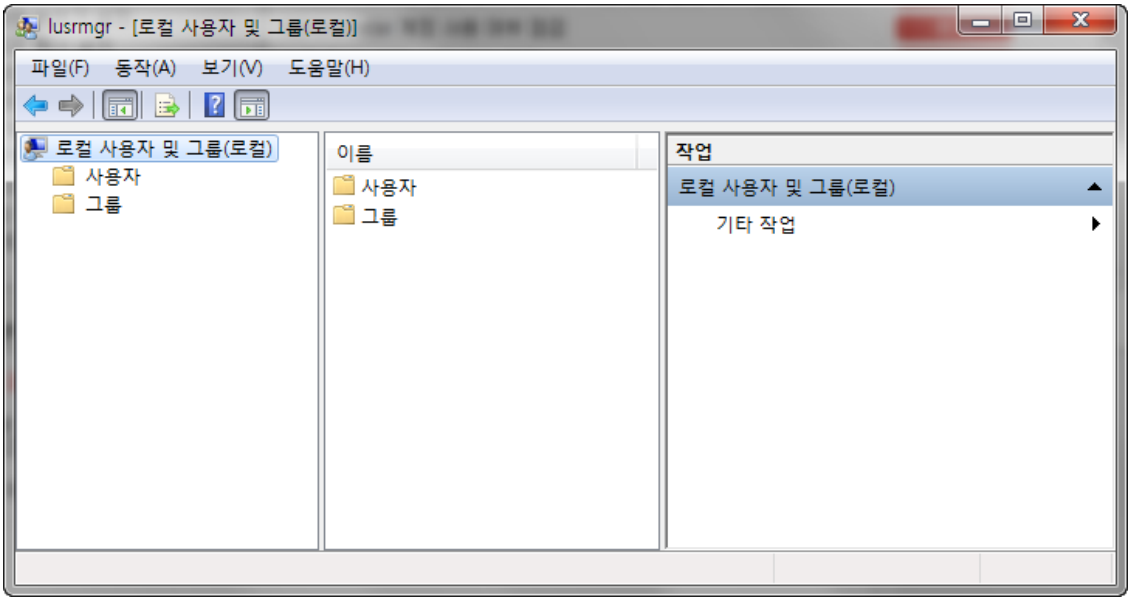
1. **점검 항목 상세 정보**에서 패스워드 사용 기간이 설정되지 않은 계정을 확인하고 **원클릭 조치**를 누릅니다.
2. 취약 계정에 패스워드 사용 기간이 설정되고, 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

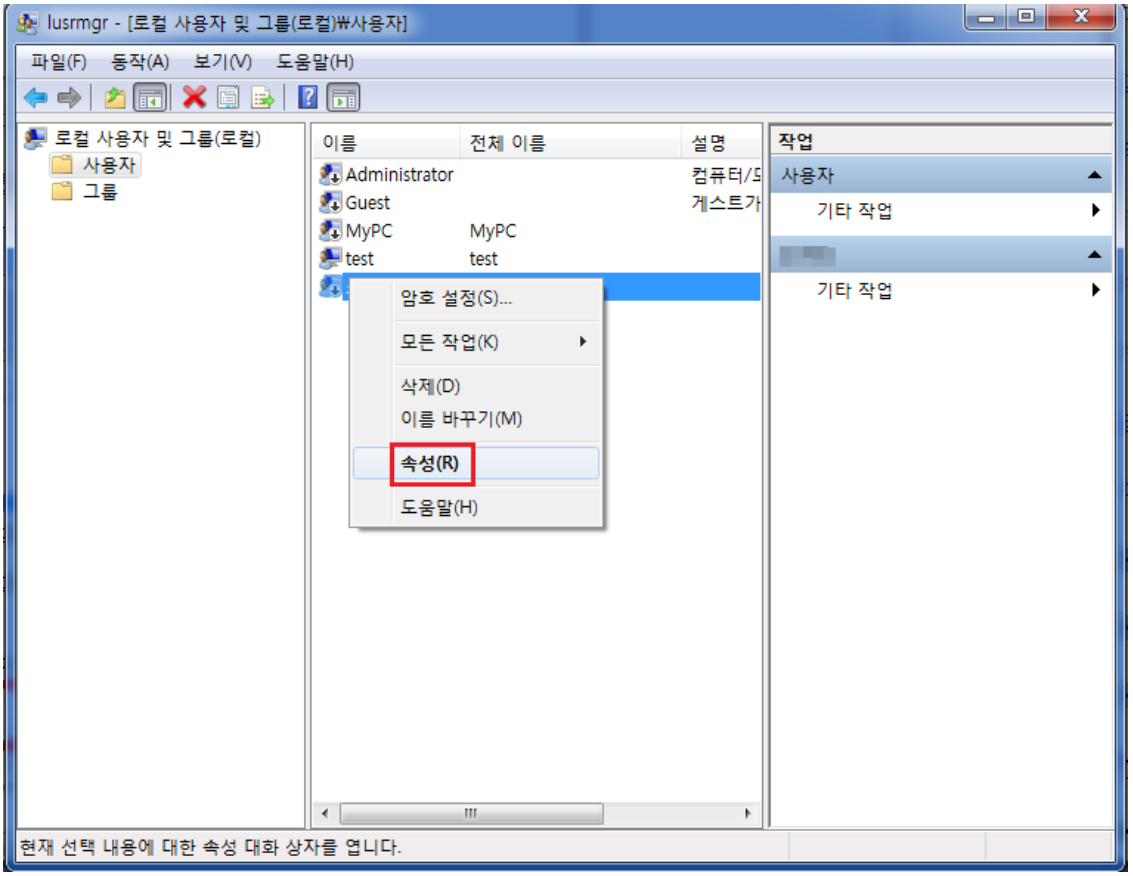
점검 결과가 **취약**인 경우, Windows Edition 의 **그룹 정책 사용 가능 여부**에 따라 각각 다른 방법으로 조치해야 합니다. Windows Edition 중 **Starter, Home, Only Core Edition** 은 그룹 정책을 사용할 수 없습니다.

그룹 정책을 사용할 수 있는 경우 (Starter, Home, Only Core 이외의 Edition)

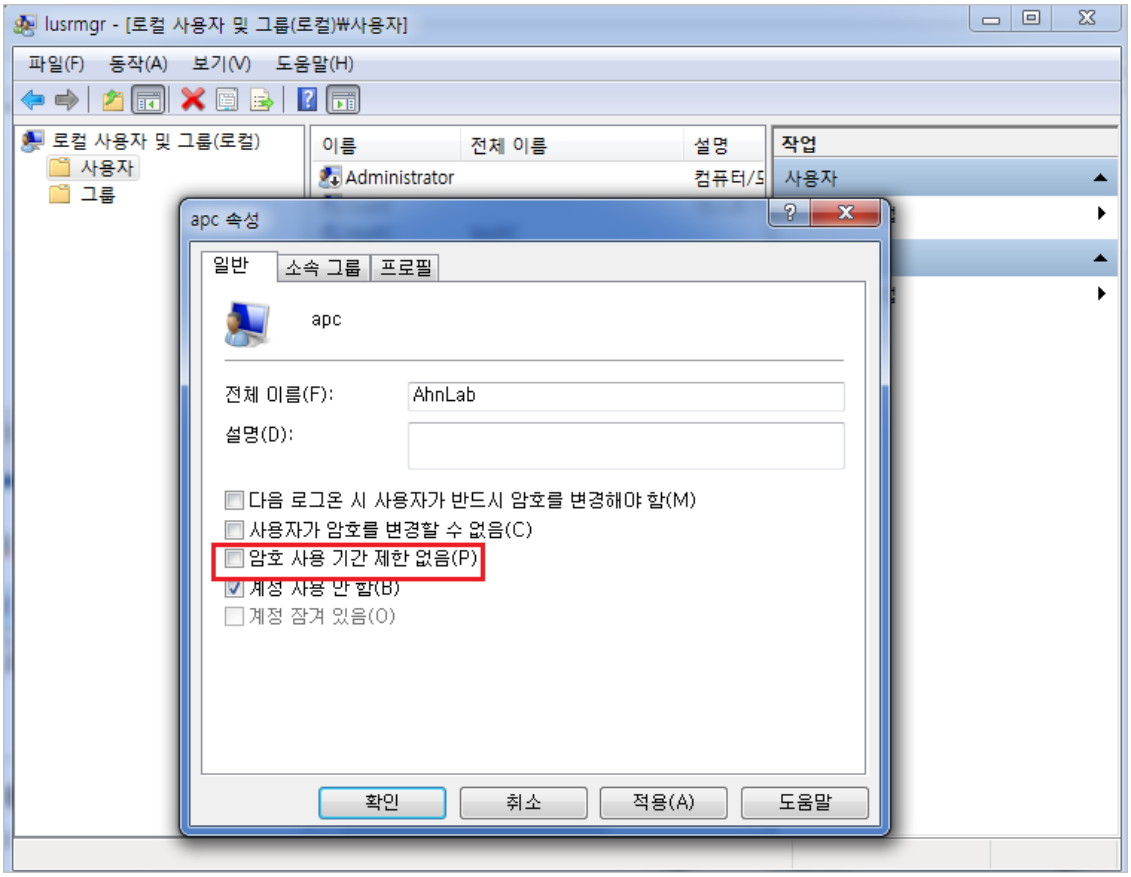
1. **제어판** > **시스템 및 보안** > **관리 도구** 에서 <**컴퓨터 관리**>를 누릅니다.
2. <컴퓨터 관리>에서 로컬 사용자 및 그룹을 관리하는 설정 창이 나타납니다.



3. 실행된 <lusrmgr - [로컬 사용자 및 그룹(로컬)]>에서 왼쪽의 폴더 중에 **사용자**를 선택합니다.
4. 패스워드 사용 기간을 설정할 계정을 선택합니다. 계정 목록에서 마우스 오른쪽 버튼을 클릭한 다음 **속성**을 누릅니다.



5. **암호 사용 기간 제한 없음** 항목을 **체크 해제** 후 **확인**을 클릭하여 설정을 종료합니다.



그룹 정책을 사용할 수 없는 경우 (Starter, Home, Only Core Edition)

1. 시작 > 모든 프로그램 > 보조 프로그램에서 명령 프롬프트를 마우스 오른쪽 버튼으로 클릭하여, 관리자 권한으로 실행합니다.
2. <명령 프롬프트>가 실행되면 다음과 같이 명령어를 입력합니다. **계정 이름**에는 **패스워드 사용 기간 제한**을 설정할 계정의 이름을 적습니다.

```
wmic useraccount where "NAME='계정 이름'" SET PassWordExpires:TRUE
```

- 계정 이름에는 패스워드 사용 기간 제한을 설정할 계정의 이름을 적습니다.

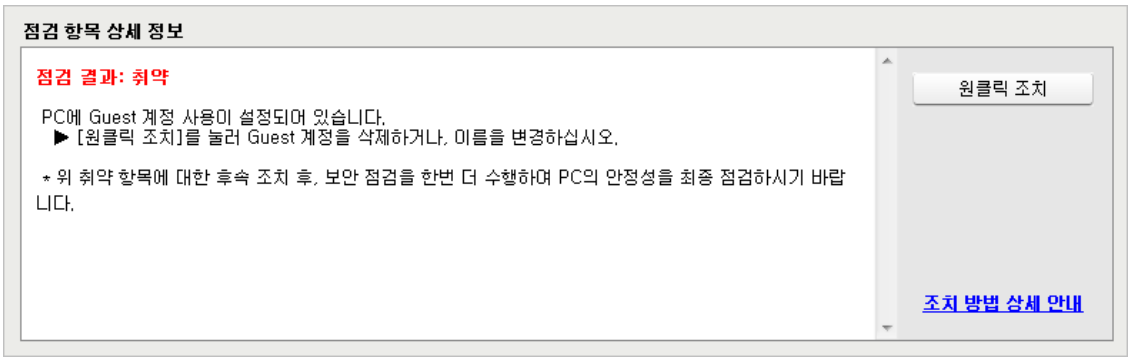
Guest 계정 사용 점검

사용자 PC 가 Guest 계정을 사용하도록 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에서 Guest 계정을 사용하지 않습니다.
- 취약: PC 에서 Guest 계정이 사용 중입니다. Guest 계정을 **사용 안 함**으로 설정하거나 **원클릭 조치**를 눌러 Guest 계정 이름을 변경하십시오.

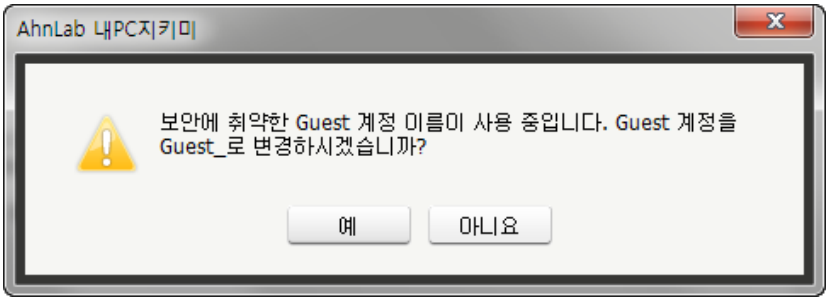


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

1. **점검 항목 상세 정보**에서 **원클릭 조치**를 누릅니다.
2. 알림 창에서 **예**를 선택하면 Guest 계정의 이름을 변경합니다. **아니요**를 선택하면 계정 이름을 변경하지 않습니다.



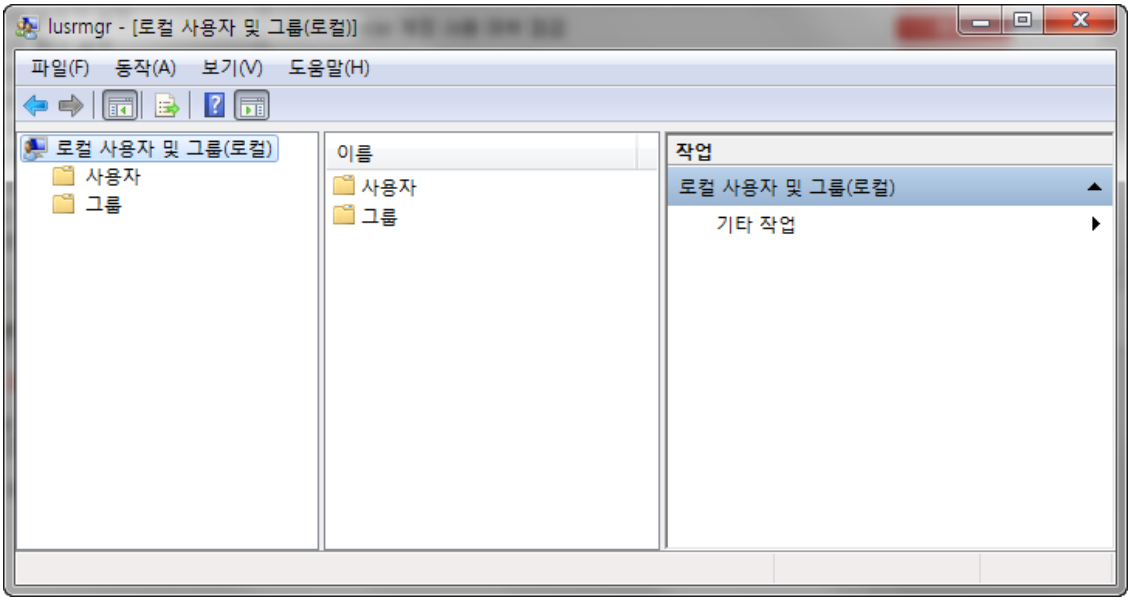
3. **예**를 선택하면 Guest 계정의 이름을 변경하고 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

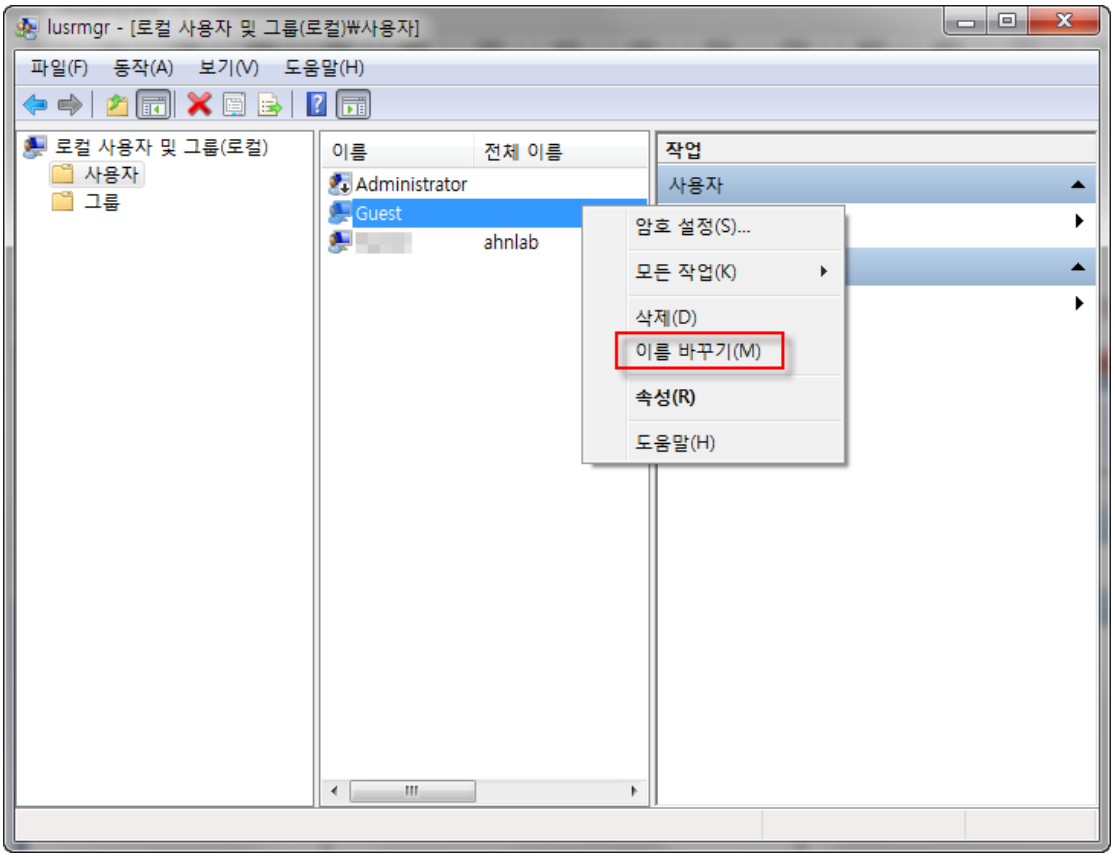
점검 결과가 **취약**인 경우, Windows Edition 의 **그룹 정책 사용 가능 여부**에 따라 각각 다른 방법으로 조치해야 합니다. Windows Edition 중 **Starter, Home, Only Core Edition** 은 그룹 정책을 사용할 수 없습니다.

그룹 정책을 사용할 수 있는 경우 (Starter, Home, Only Core 이외의 Edition)

1. **제어판** > **시스템 및 보안** > **관리 도구** 에서 <**컴퓨터 관리**>를 누릅니다.
2. <컴퓨터 관리>에서 로컬 사용자 및 그룹을 관리하는 설정 창이 나타납니다.



3. **로컬 사용자 및 그룹** > **사용자**를 클릭합니다. 목록에서 **Guest** 계정을 확인한 후, 마우스 오른쪽 버튼을 클릭하여 **계정을 삭제**하거나 **이름을 변경**해야 합니다.



그룹 정책을 사용할 수 없는 경우 (Starter, Home, Only Core Edition)

1. 시작 > 모든 프로그램 > 보조 프로그램에서 명령 프롬프트를 마우스 오른쪽 버튼으로 클릭하여, 관리자 권한으로 실행합니다.
2. <명령 프롬프트>가 실행되면 다음과 같이 명령어를 입력합니다.

```
wmic useraccount where "NAME='Guest'" CALL RENAME NAME='변경 이름'
```

- **변경 이름**에는 **Guest** 계정의 변경될 이름을 적습니다.

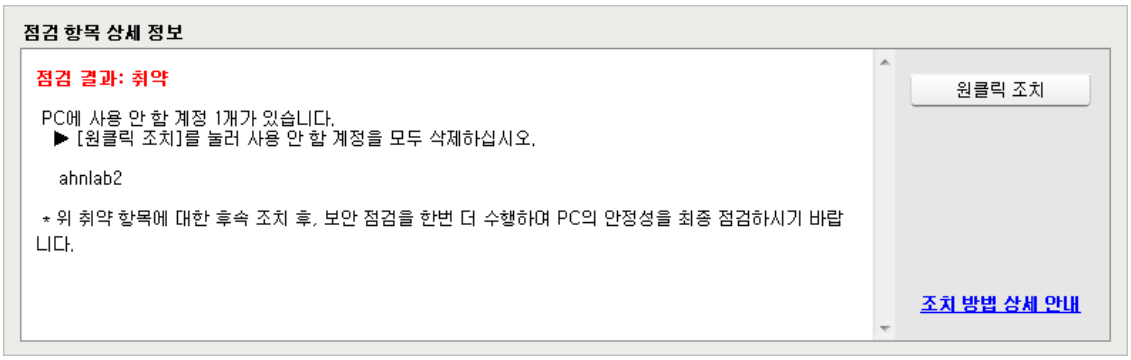
사용 안 함 계정 점검

사용자 PC 에 사용하지 않는 계정이 삭제되지 않고 남아 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 **사용 안 함** 계정이 존재하지 않습니다.
- 취약: PC 에 **사용 안 함**으로 설정된 계정의 개수가 나타납니다. **원클릭 조치**를 눌러 사용 안 함 계정을 삭제하십시오.

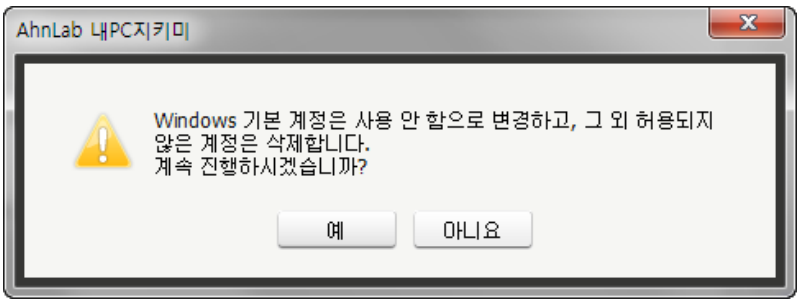


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

1. **점검 항목 상세 정보**에서 **원클릭 조치**를 누릅니다.
2. 알림 창에서 **예**를 선택하면 Windows 기본 계정은 사용 안 함으로 변경하고, 그 외 계정은 삭제합니다. **아니요**를 선택하면 계정 정보를 변경하지 않습니다.



3. 알림 창에서 **예**를 선택하면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

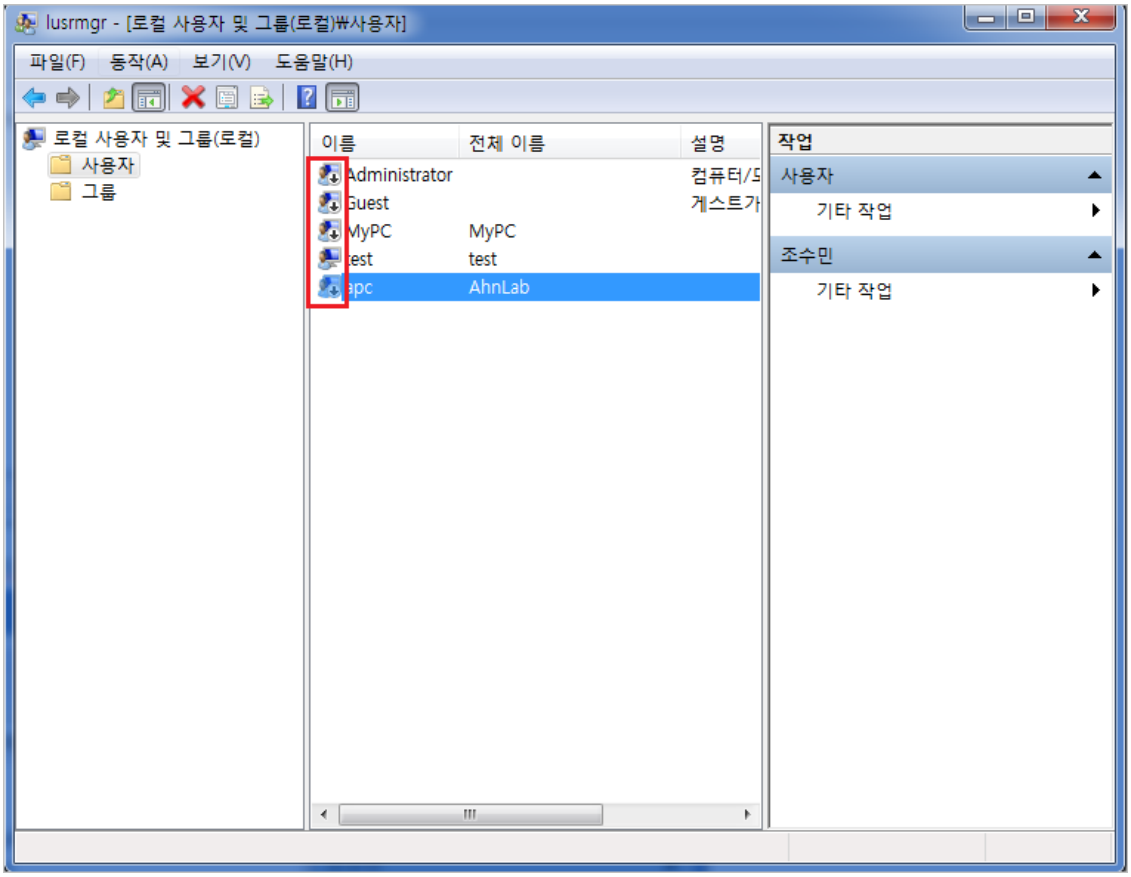
점검 결과가 **취약**인 경우, Windows Edition 의 **그룹 정책 사용 가능 여부**에 따라 각각 다른 방법으로 조치해야 합니다. Windows Edition 중 **Starter, Home, Only Core Edition** 은 그룹 정책을 사용할 수 없습니다.

그룹 정책을 사용할 수 있는 경우 (Starter, Home, Only Core 이외의 Edition)

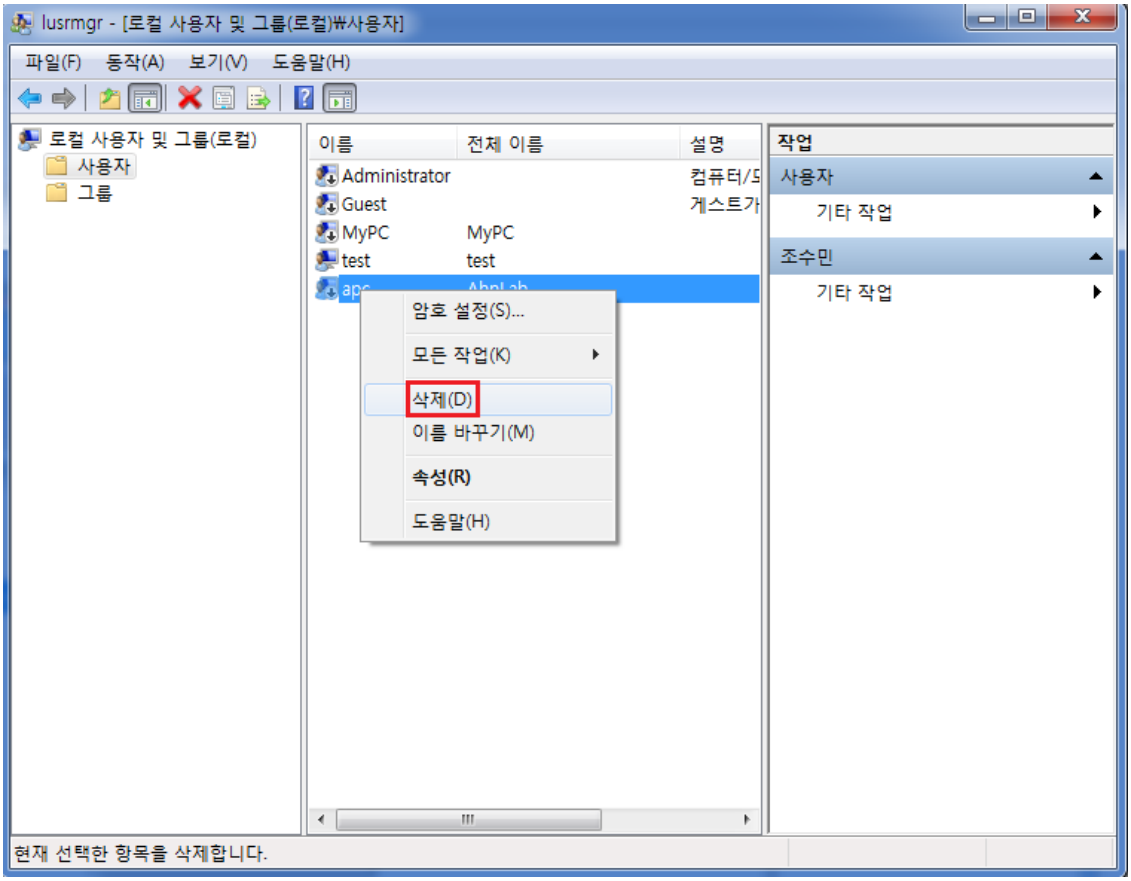
가. 사용 안 함 계정 삭제

1. **제어판** > **시스템 및 보안** > **관리 도구** 에서 <**컴퓨터 관리**>를 누릅니다.

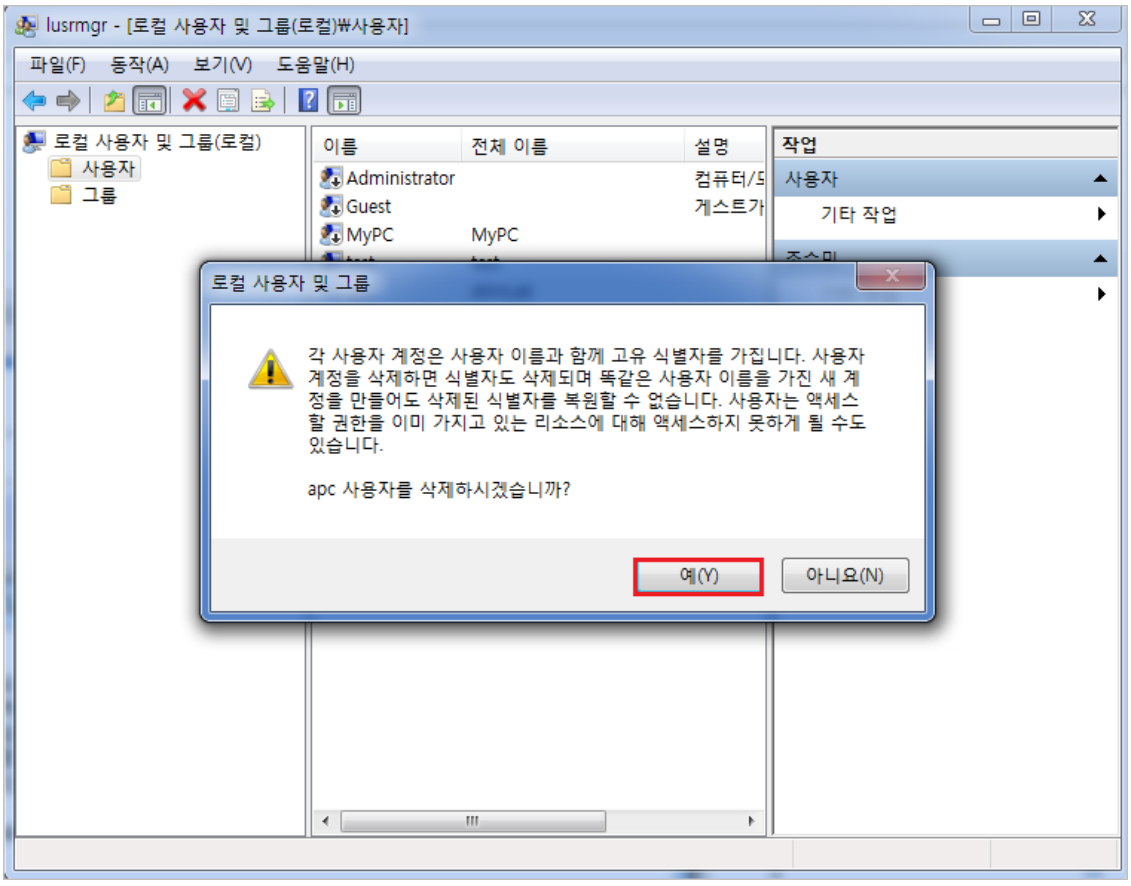
2. <컴퓨터 관리>에서 로컬 사용자 및 그룹을 관리하는 설정 창이 나타납니다.
3. **로컬 사용자 및 그룹** > **사용자**에서 좌측 아이콘에 **아래쪽 화살표 모양 표시 ↓**가 나타난 계정 목록을 확인합니다.



4. 해당 계정을 선택한 후, 마우스 오른쪽 버튼을 클릭하여 **삭제**를 누릅니다.

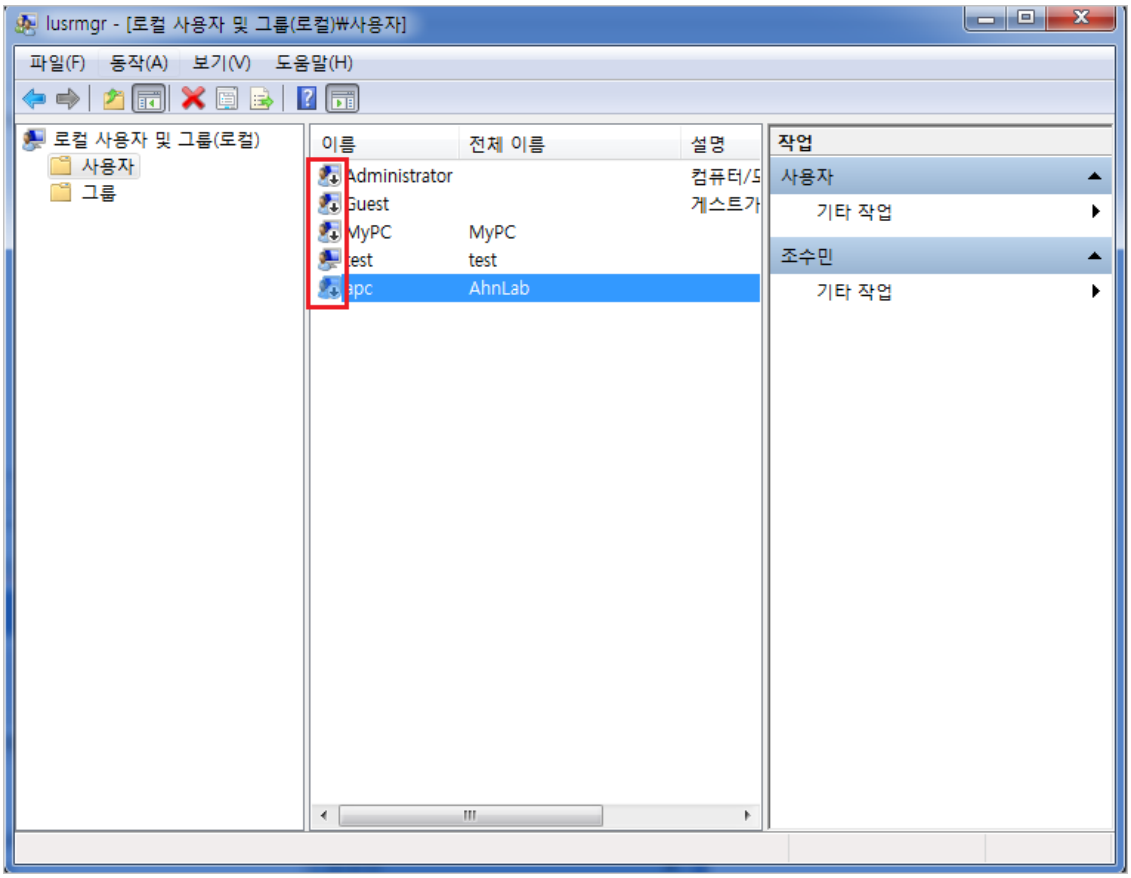


5. **예**를 클릭하여 사용 안 함 계정을 삭제합니다.

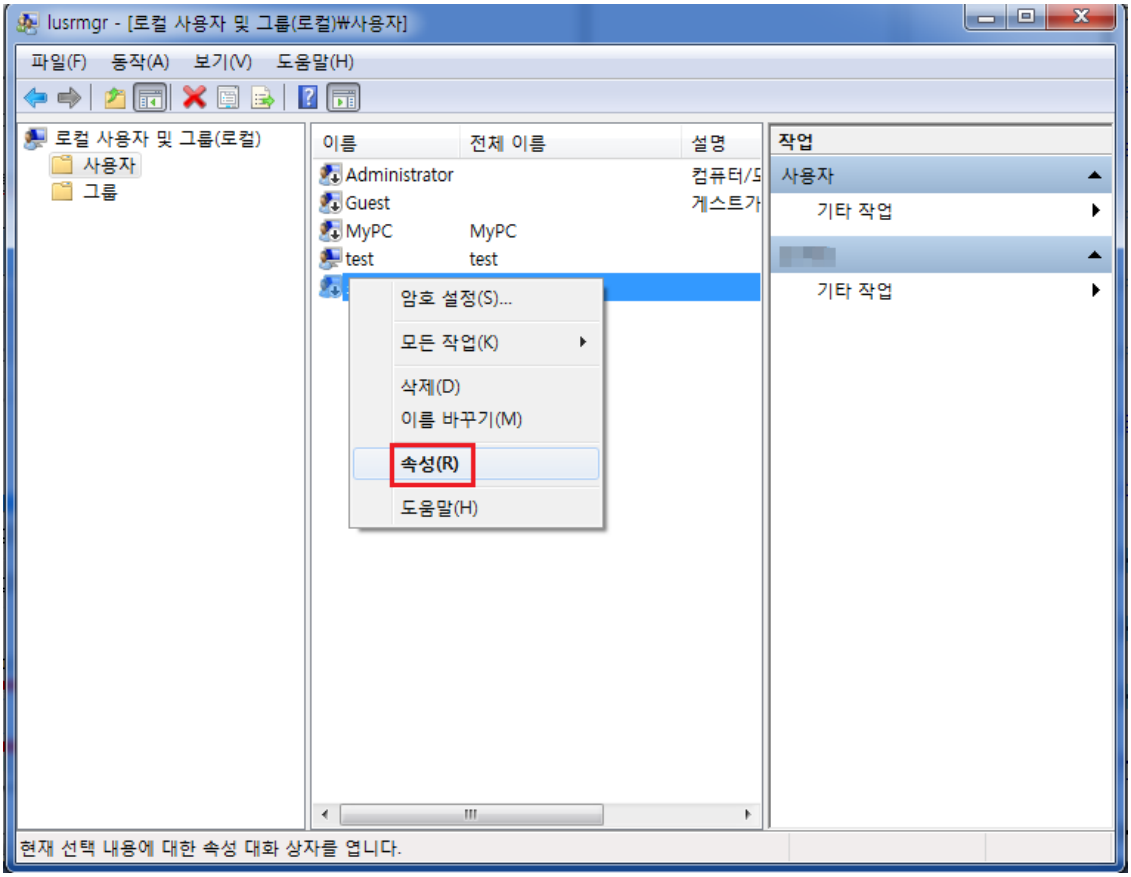


나. 사용 안 함 계정을 사용하도록 변경하기

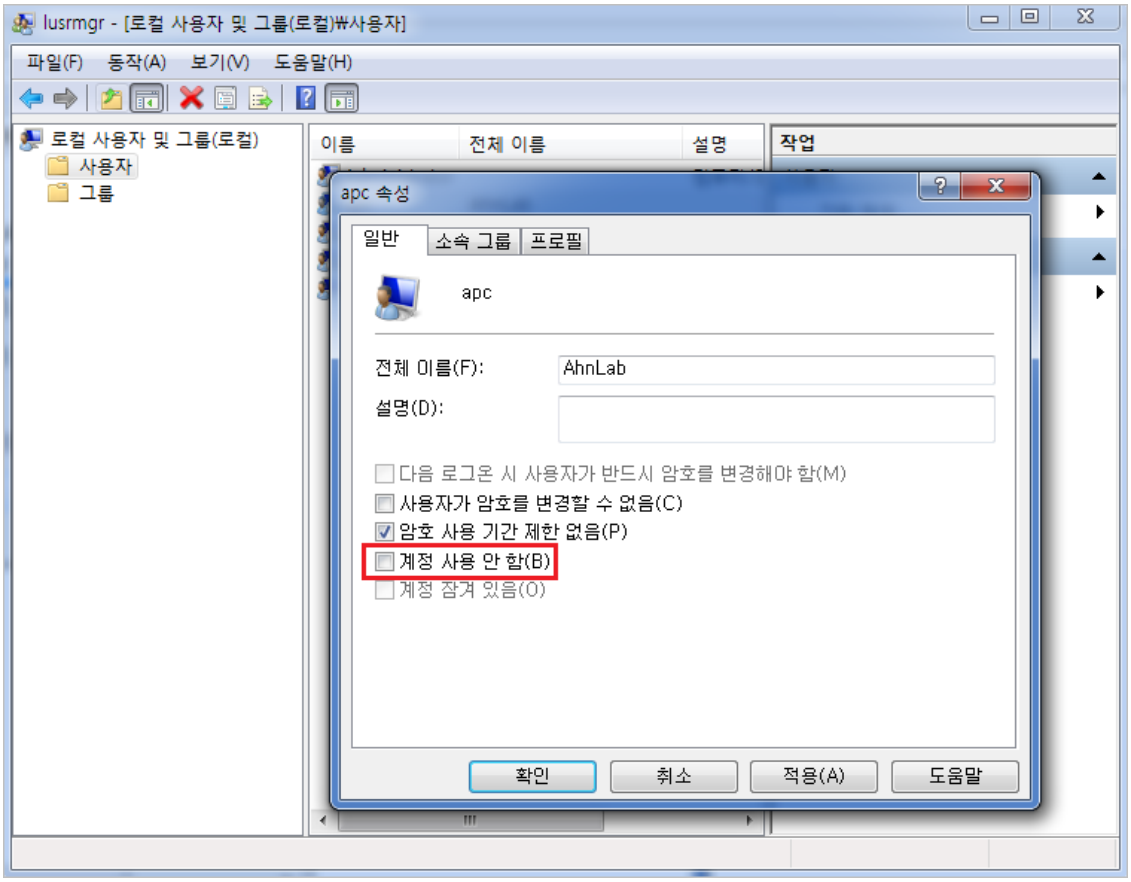
1. **제어판** > **시스템 및 보안** > **관리 도구** 에서 <**컴퓨터 관리**>를 누릅니다.
2. <컴퓨터 관리>에서 로컬 사용자 및 그룹을 관리하는 설정 창이 나타납니다.
3. **로컬 사용자 및 그룹** > **사용자**에서 좌측 아이콘에 **아래쪽 화살표 모양 표시** ↓가 나타난 계정 목록을 확인합니다.



4. 활성화할 계정을 선택한 후, 마우스 오른쪽 버튼을 클릭하여 **속성**을 누릅니다.



5. **계정 사용 안 함**의 체크를 해제하고 **확인**을 클릭하여 해당 계정을 사용하도록 설정합니다.



그룹 정책을 사용할 수 없는 경우 (Starter, Home, Only Core Edition)

1. 시작 > 모든 프로그램 > 보조 프로그램에서 명령 프롬프트를 마우스 오른쪽 버튼으로 클릭하여, 관리자 권한으로 실행합니다.
2. <명령 프롬프트>가 실행되면 다음과 같이 명령어를 입력합니다.

   net user *계정 이름* /active:yes

   - **계정 이름**에는 계정을 활성화할 **사용 안 함** 계정의 이름을 적습니다.

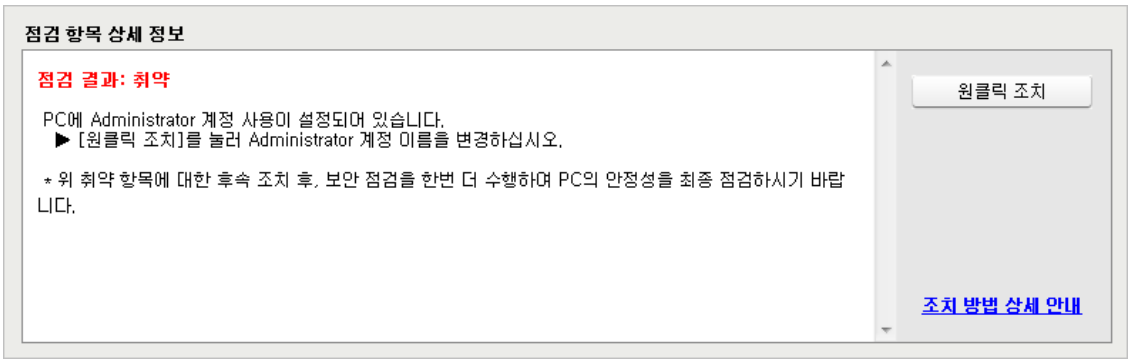
Administrator 계정 사용 점검

사용자 PC 가 Administrator 계정을 사용하도록 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 Administrator 계정이 존재하지 않습니다.
- 취약: PC 에 Administrator 계정이 사용 중으로 나타납니다. **원클릭 조치**를 눌러 관리 Administrator 계정 이름을 변경하십시오.

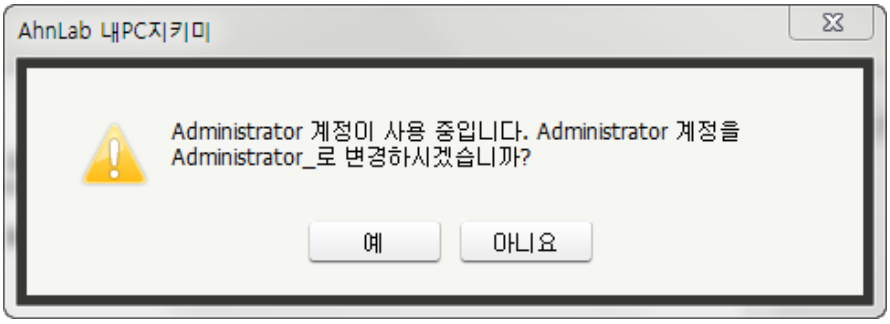


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

1. **점검 항목 상세 정보**에서 **원클릭 조치**를 누릅니다.
2. 알림 창에서 **예**를 선택하면 Administrator계정의 이름이 변경되며, **아니요**를 선택하면 계정 정보를 변경하지 않습니다.



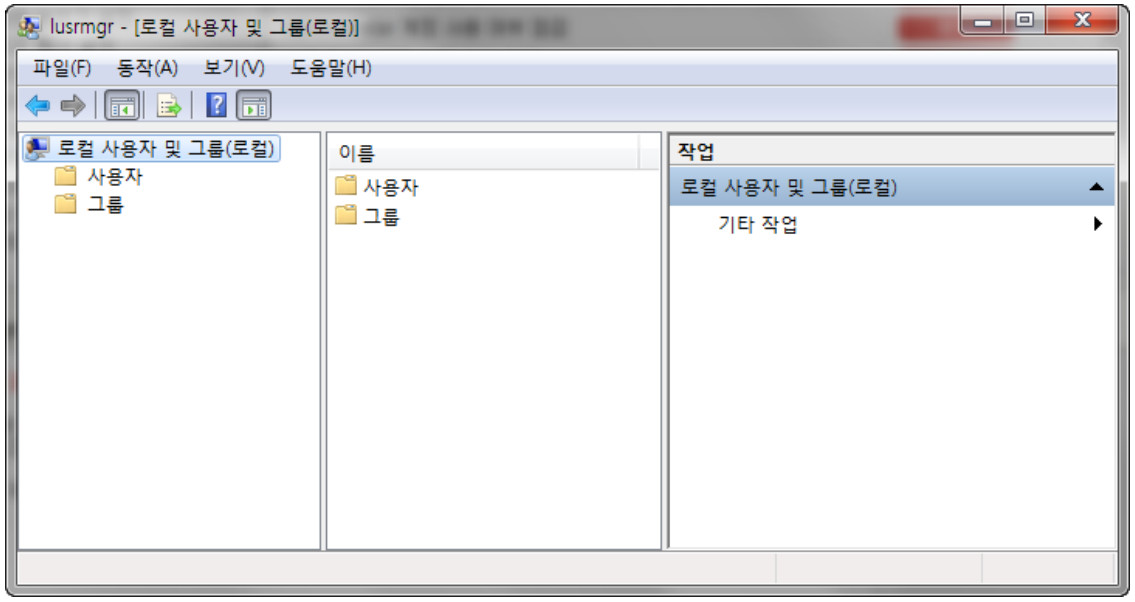
3. 알림 창에서 **예**를 선택하면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

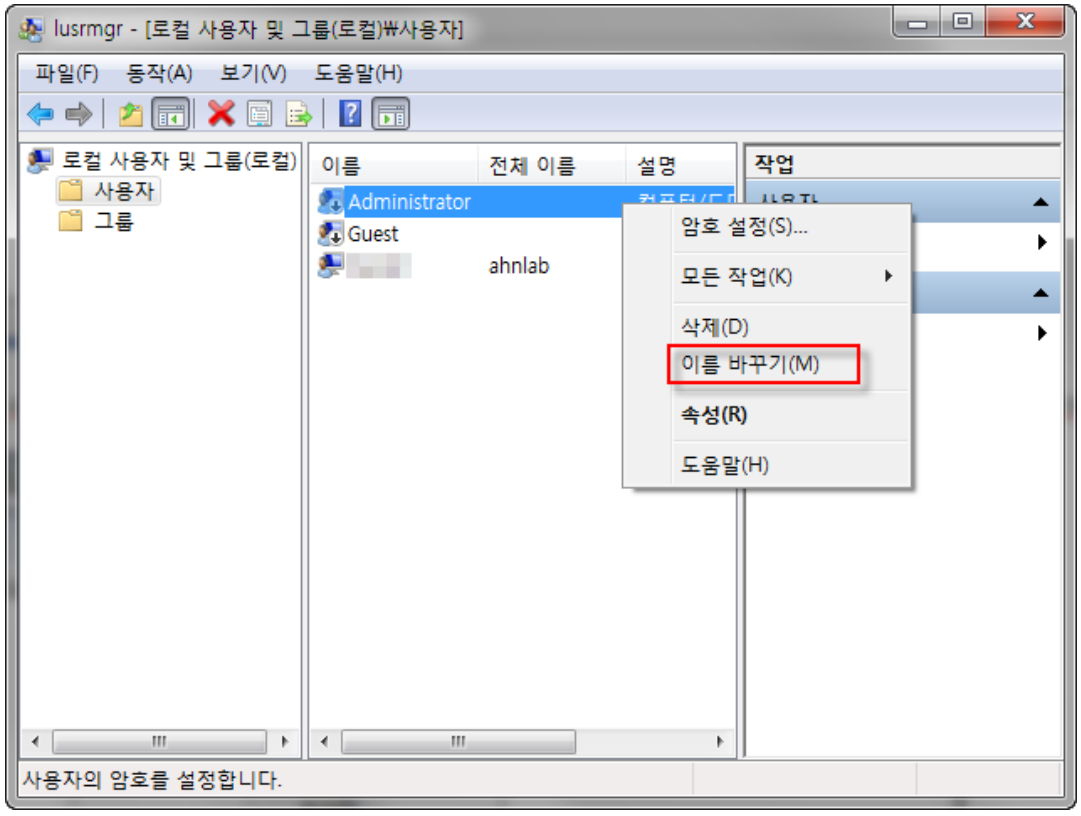
점검 결과가 **취약**인 경우, Windows Edition 의 **그룹 정책 사용 가능 여부**에 따라 각각 다른 방법으로 조치해야 합니다. Windows Edition 중 **Starter, Home, Only Core Edition** 은 그룹 정책을 사용할 수 없습니다.

그룹 정책을 사용할 수 있는 경우 (Starter, Home, Only Core 이외의 Edition)

1. **제어판** > **시스템 및 보안** > **관리 도구** 에서 <**컴퓨터 관리**>를 누릅니다.
2. <컴퓨터 관리>에서 로컬 사용자 및 그룹을 관리하는 설정 창이 나타납니다.



3. **로컬 사용자 및 그룹** > **사용자**를 클릭합니다. 목록에서 **Administrator** 계정을 확인한 후, 마우스 오른쪽 버튼을 클릭하여 **계정을 삭제**하거나 **이름을 변경**해야 합니다.



그룹 정책을 사용할 수 없는 경우 (Starter, Home, Only Core Edition)

1. 시작 > 모든 프로그램 > 보조 프로그램에서 명령 프롬프트를 마우스 오른쪽 버튼으로 클릭하여, 관리자 권한으로 실행합니다.
2. <명령 프롬프트>가 실행되면 다음과 같이 명령어를 입력합니다.

```
wmic useraccount where "NAME='Administrator'" CALL RENAME NAME='변경 이름'
```

- **변경 이름**에는 **Administrator** 계정의 변경될 이름을 적습니다.

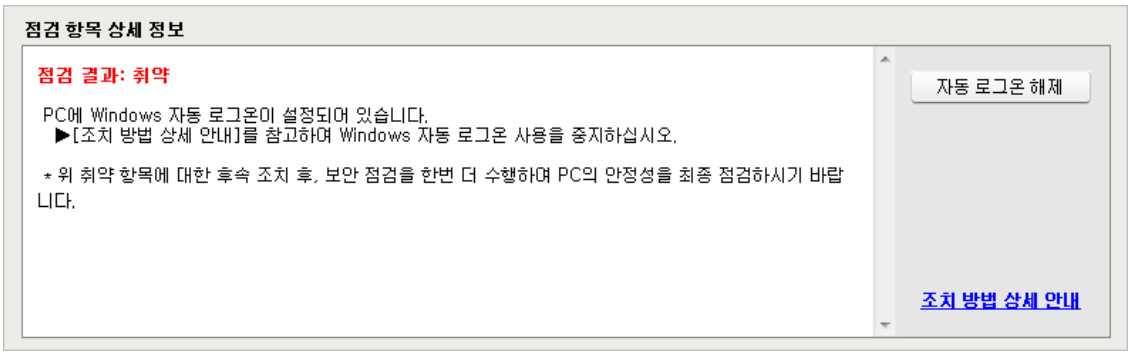
Windows 자동 로그온 점검

윈도우의 사용자 계정에 비밀번호를 입력하지 않고 자동으로 로그온 하도록 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 Windows 자동 로그온이 설정되어 있지 않습니다.
- 취약: PC 에 Windows 자동 로그온 기능이 설정되어 있습니다. **자동 로그온 해제** 버튼을 눌러 Windows 자동 로그온 설정을 해제하십시오.

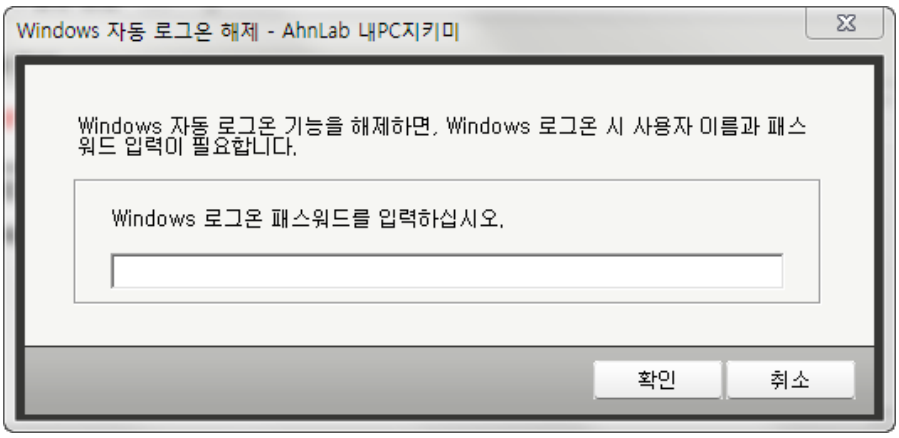


조치 방법

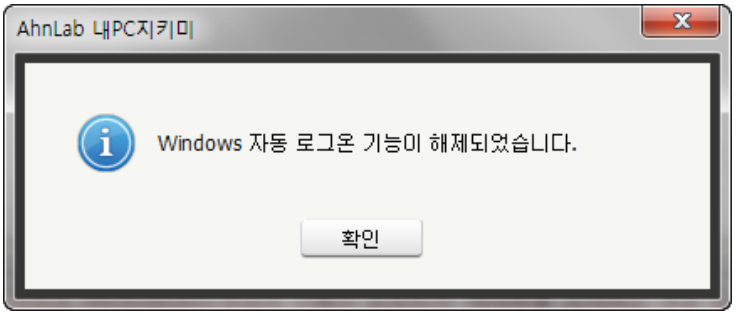
Windows 자동 로그온 기능을 해제하는 방법은 점검 항목 상세 정보에서 **자동 로그온 해제** 버튼을 누르거나 **사용자 조치**를 통해 설정을 해제할 수 있습니다.

[자동 로그온 해제]

1. **점검 항목 상세 정보**에서 **자동 로그온 해제**를 누릅니다.
2. 자동 로그온 해제를 위해 다음의 화면에서 Windows 로그온 패스워드를 입력하고 확인을 누릅니다.



3. Windows 자동 로그온 기능 해제 알림 창이 나타납니다.



4. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

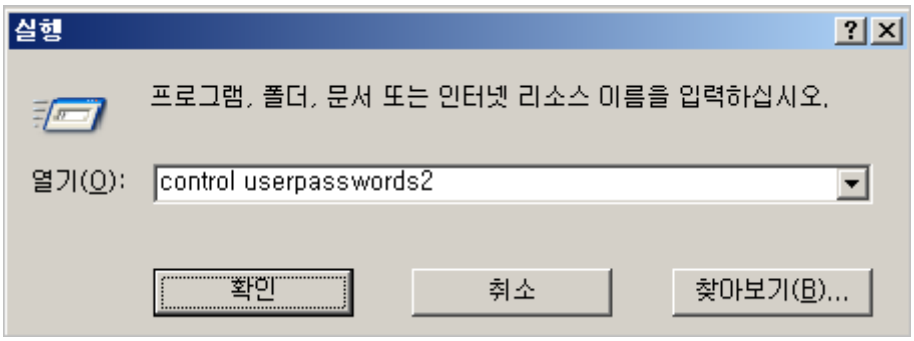
[사용자 조치]

윈도우의 사용자 계정에 자동으로 로그온 하도록 설정된 경우 다음과 같은 방법으로 설정을 해제할 수 있습니다.
사용자 계정을 통한 설정 변경과 레지스트리 수정/삭제를 통한 설정 변경이 있습니다.

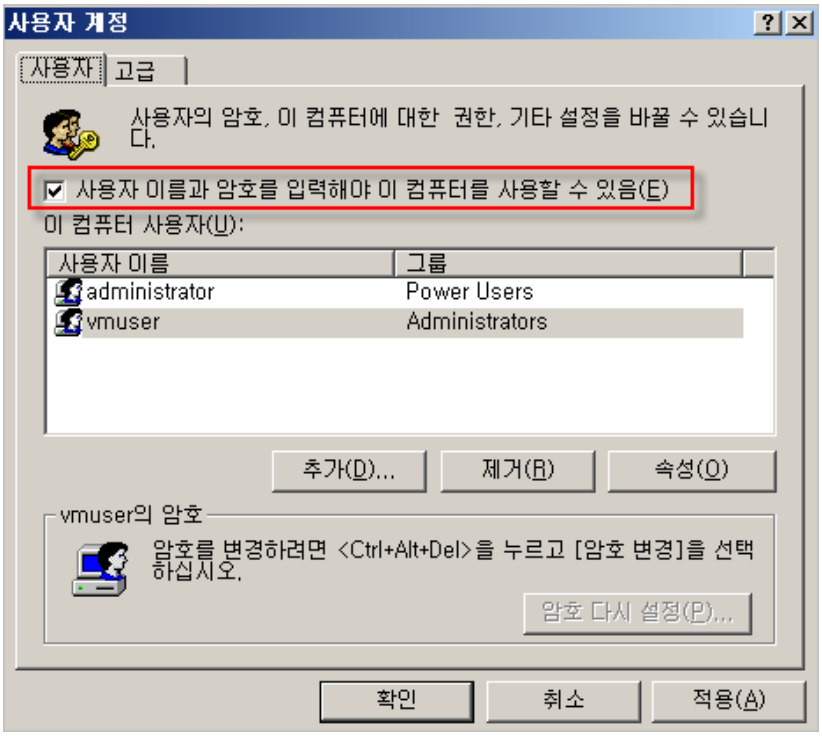
가. 사용자 계정을 통한 설정 변경

Windows 2003 이하

1. 윈도우 + R키를 눌러 실행 창을 띄운 후 **control userpasswords2**를 입력합니다.

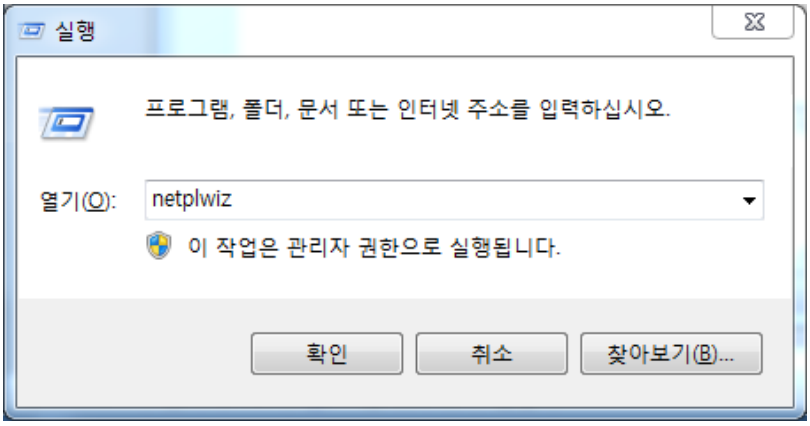


2. **사용자 이름과 암호를 입력해야 이 컴퓨터를 사용할 수 있음**을 체크 후 확인을 클릭합니다.

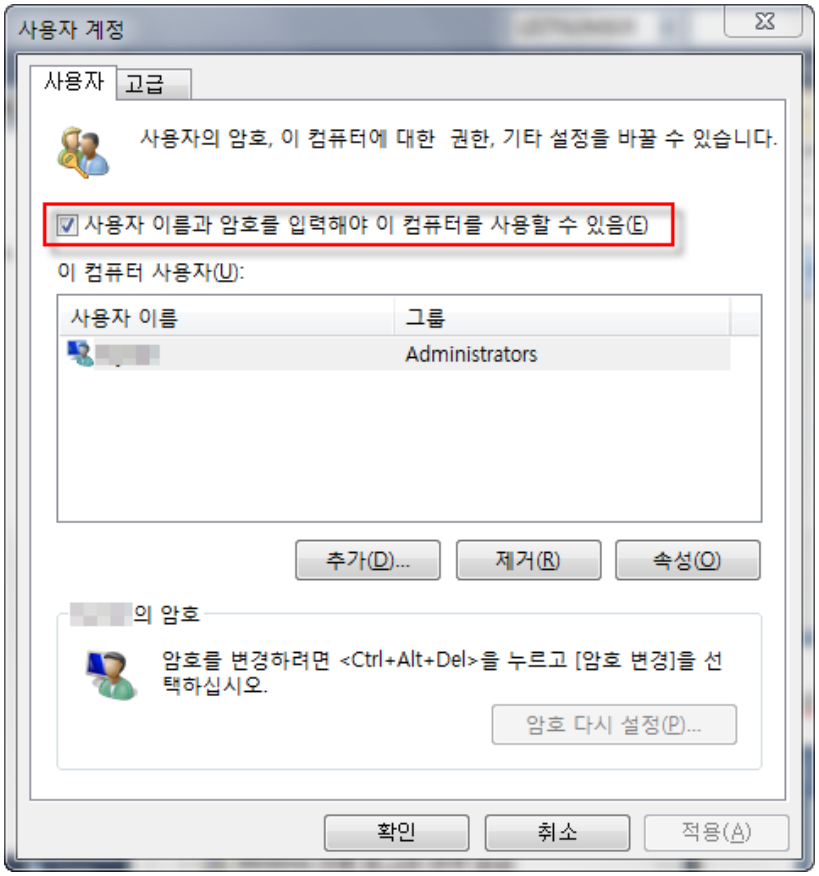


Vista 이상

1. 윈도우 + R 키를 눌러 실행 창을 띄운 후 **netplwiz** 를 입력합니다.

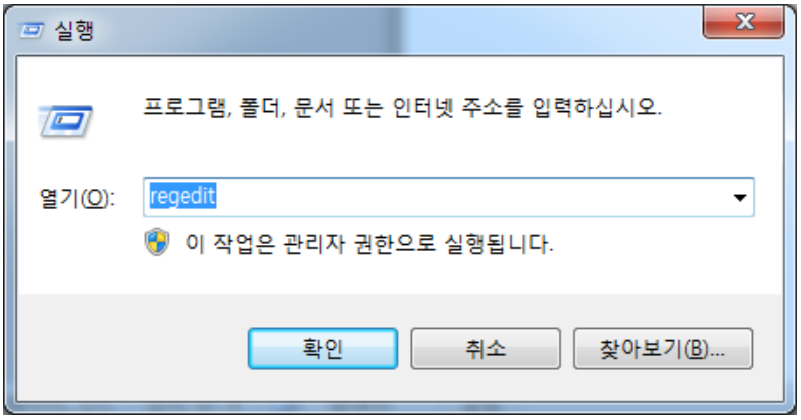


2. **사용자 이름과 암호를 입력해야 이 컴퓨터를 사용할 수 있음**을 체크 후 확인을 클릭합니다.

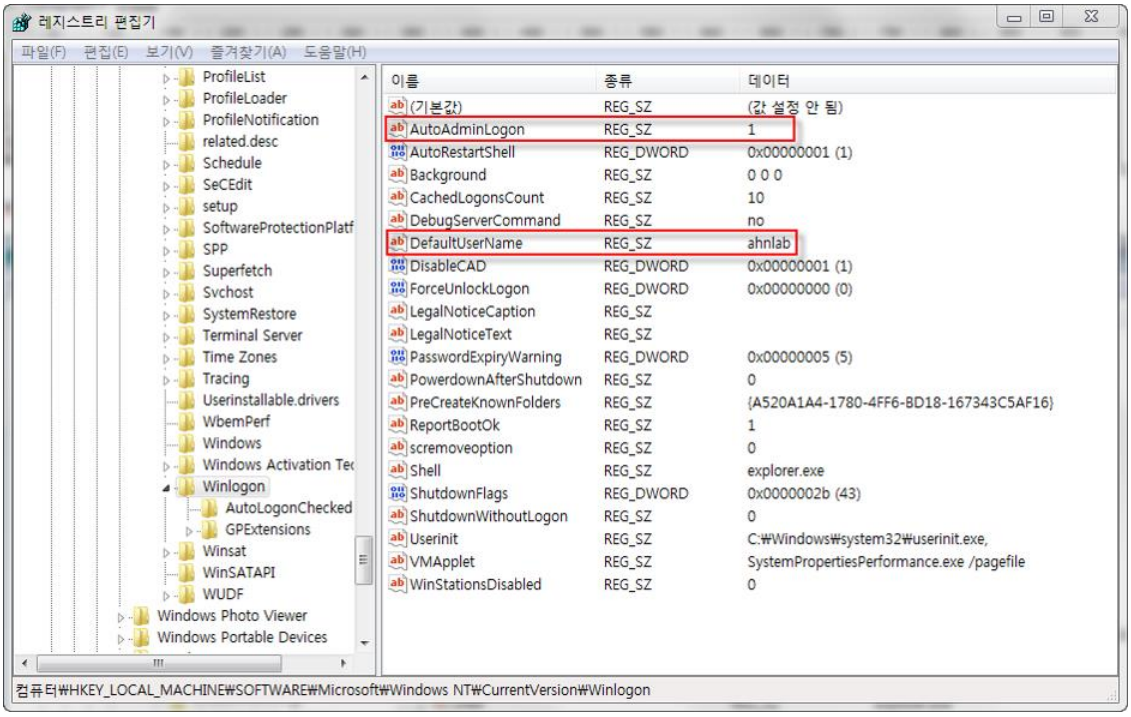


나. 레지스트리 수정/삭제를 통한 설정 변경

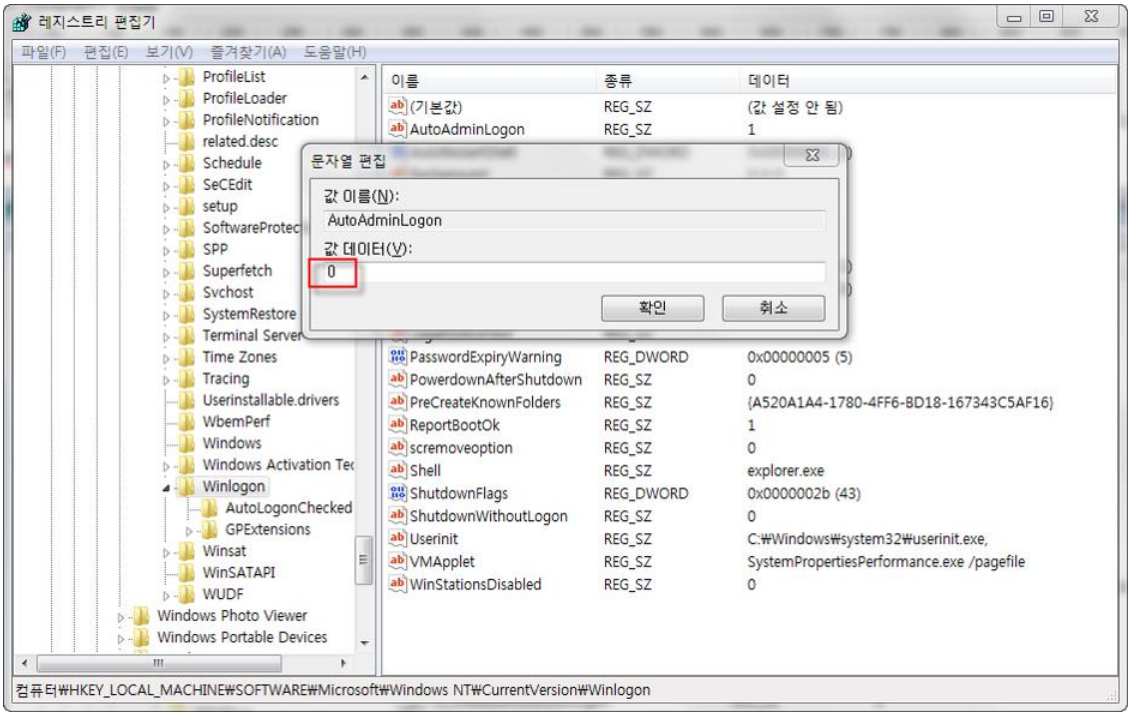
1. 윈도우 + R 키를 눌러 실행 창을 띄운 후 **regedit** 를 입력합니다.



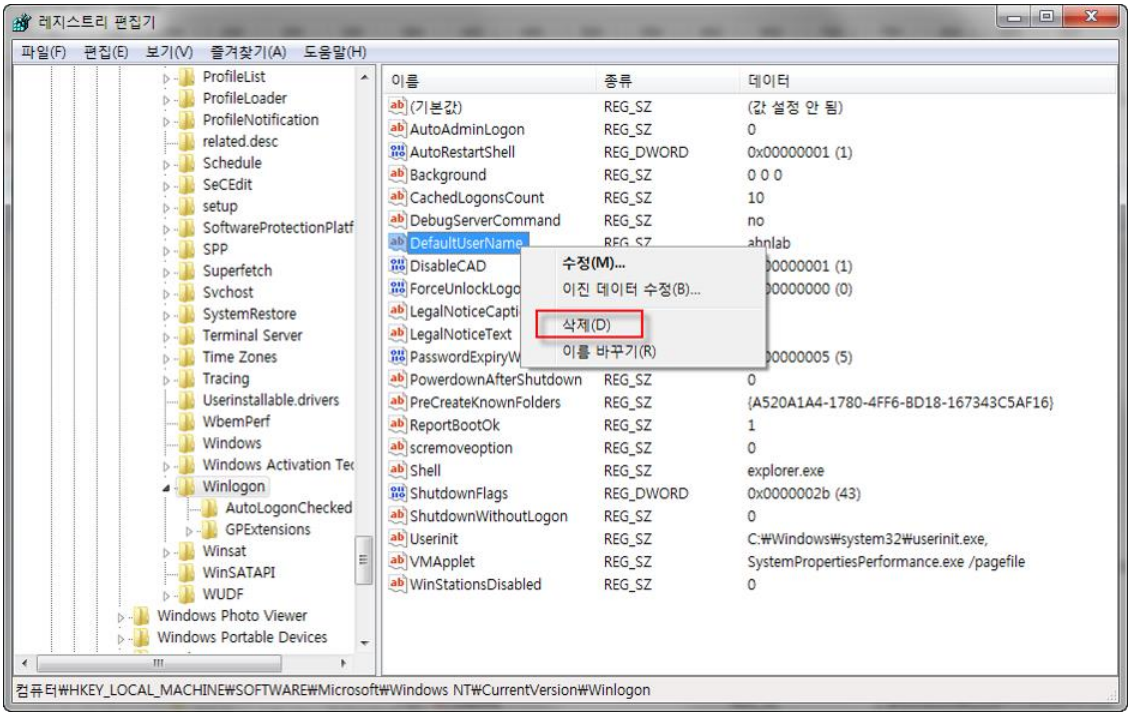
2. **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon** 으로 이동하여 **AutoAdminLogon** 값과 **DefaultUserName** 값을 확인합니다.



3. **AutoAdminLogon** 값을 더블 클릭하여 0 으로 편집한 후 확인을 클릭합니다.



4. **DefaultUserName** 값을 우클릭한 후 삭제를 클릭합니다.


레지스트리 편집기
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)
ProfileList
ProfileLoader
ProfileNotification
related.desc
Schedule
SeCEdit
setup
SoftwareProtectionPlatf
SPP
Superfetch
Svchost
SystemRestore
Terminal Server
Time Zones
Tracing
Userinstallable.drivers
WbemPerf
Windows
Windows Activation Tec
Winlogon
AutoLogonChecked
GPExtensions
Winsat
WinSATAPI
WUDF
Windows Photo Viewer
Windows Portable Devices
이름 종류 데이터
(기본값) REG_SZ (값 설정 안 됨)
AutoAdminLogon REG_SZ 0
AutoRestartShell REG_DWORD 0x00000001 (1)
Background REG_SZ 0 0 0
CachedLogonsCount REG_SZ 10
DebugServerCommand REG_SZ no
DefaultUserName REG_SZ ahnlab
DisableCAD
ForceUnlockLogo
LegalNoticeCapti
LegalNoticeText
PasswordExpiryW
수정(M)...
이진 데이터 수정(B)...
삭제(D)
이름 바꾸기(R)
PowerdownAfterShutdown REG_SZ 0
PreCreateKnownFolders REG_SZ {A520A1A4-1780-4FF6-BD18-167343C5AF16}
ReportBootOk REG_SZ 1
scremoveoption REG_SZ 0
Shell REG_SZ explorer.exe
ShutdownFlags REG_DWORD 0x0000002b (43)
ShutdownWithoutLogon REG_SZ 0
Userinit REG_SZ C:₩Windows₩system32₩userinit.exe,
VMApplet REG_SZ SystemPropertiesPerformance.exe /pagefile
WinStationsDisabled REG_SZ 0
컴퓨터₩HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon

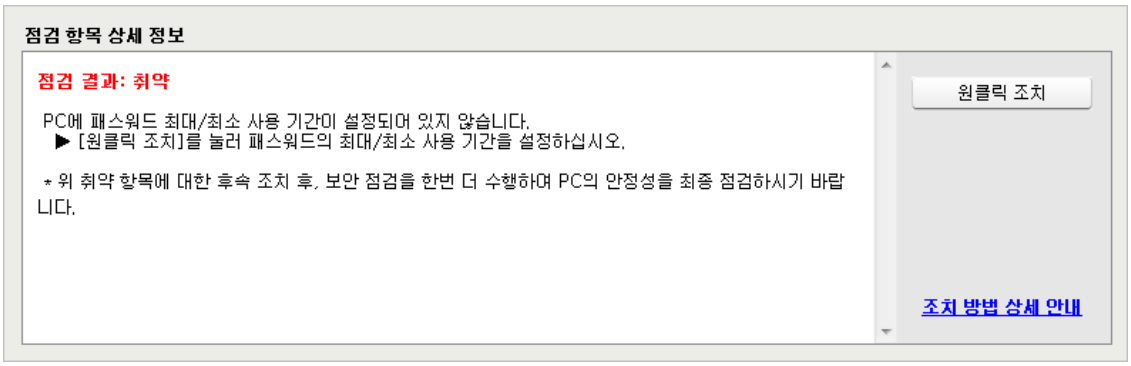
패스워드 최대/최소 사용 기간 설정 점검

패스워드에 최대/최소 사용 기간이 설정되어 있는지 여부를 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 의 암호 정책에서 패스워드 최대/최소 사용 기간이 설정되어 있습니다.
- 취약: PC 의 암호 정책에서 패스워드 사용 기간이 설정되어 있지 않습니다. **원클릭 조치**를 눌러 패스워드의 최대/최소 사용 기간을 설정하십시오.

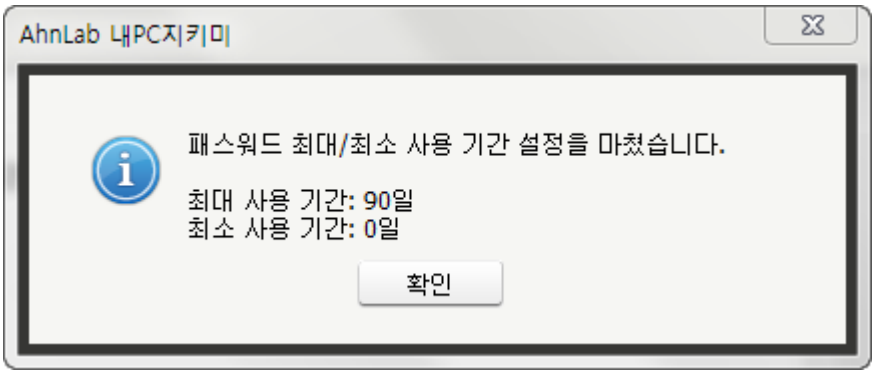


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. 관리자가 설정한 패스워드 최대/최소 사용 기간이 설정되면 다음과 같은 알림 창이 나타납니다.

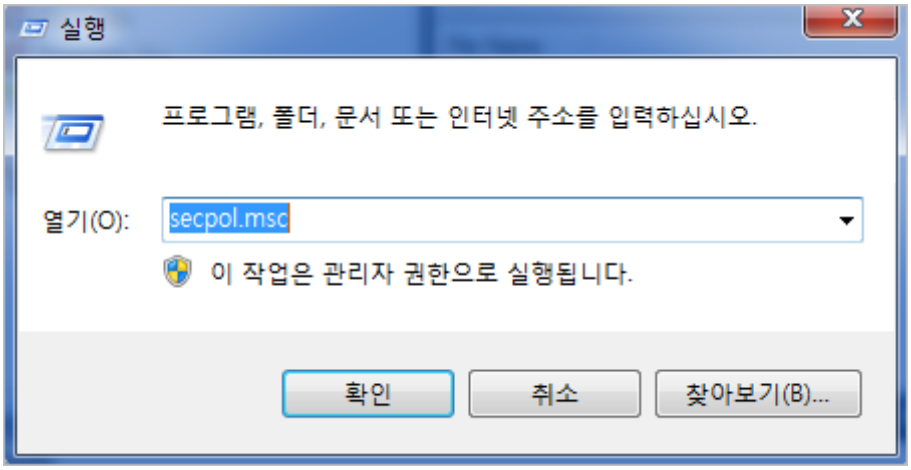


3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

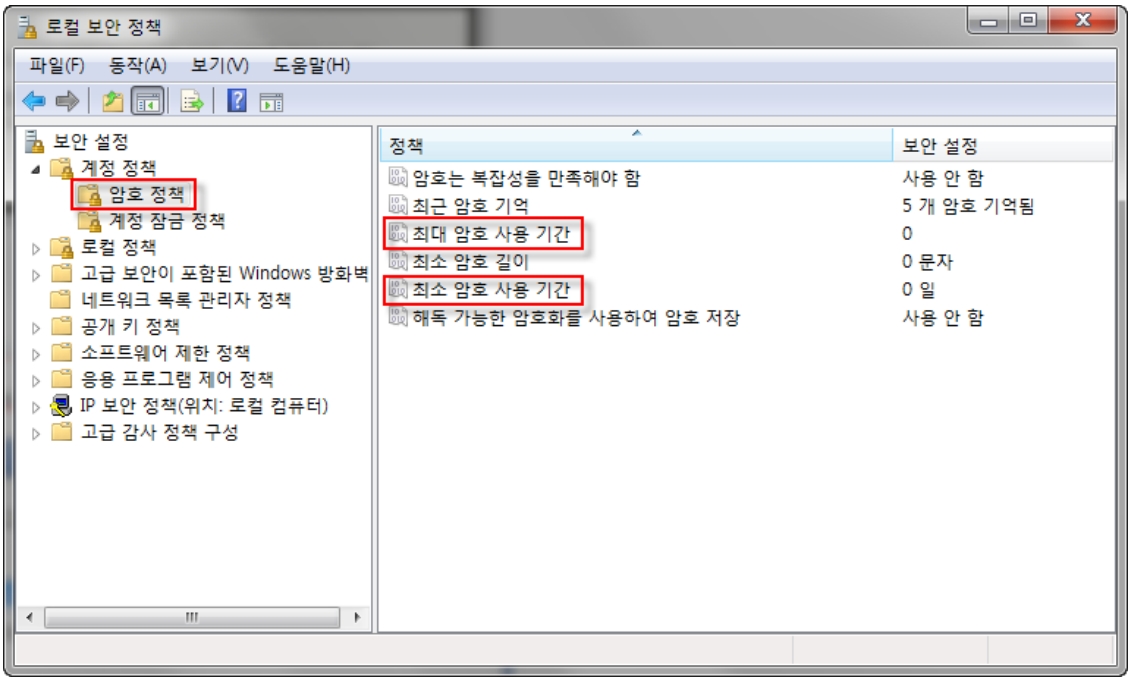
[사용자 조치]

패스워드 최대/최소 사용 기간의 설정을 확인하는 방법은 다음과 같습니다.

1. 윈도우 + R 키를 눌러 실행 창을 띄운 후 **secpol.msc** 를 입력합니다.



2. **계정 정책** > **암호 정책**을 클릭한 후 정책 목록을 확인합니다.



3. 최대 암호 사용 기간과 최소 암호 사용 기간이 설정되어 있는지 확인합니다.

참고

제품 점검 항목 상세 정보의 오른쪽에 있는 **원클릭 조치** 버튼을 눌러 해당 취약 점검 항목에 대한 빠른 후속 조치를 할 수 있습니다.

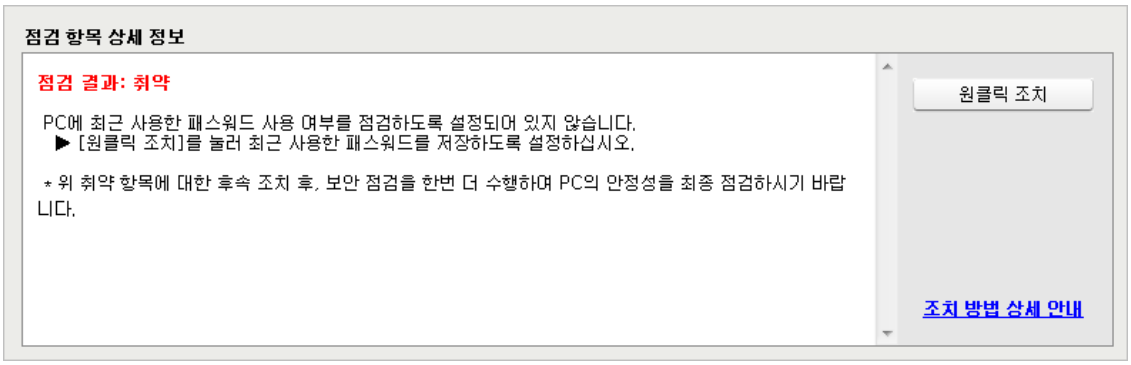
최근 사용한 패스워드 사용 점검

사용자 PC 에서 최근 사용한 패스워드를 사용하고 있는지 여부를 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 최근 사용한 패스워드 사용 여부를 점검하도록 설정되어 있습니다.
- 취약: PC 에 최근 사용한 패스워드 사용 여부를 점검하도록 설정되어 있지 않습니다. **원클릭 조치**를 눌러 최근 사용한 패스워드를 저장하도록 설정하십시오.

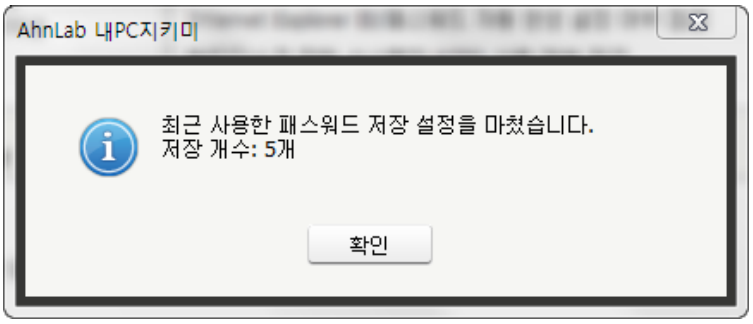


조치 방법

원클릭 조치 버튼을 통해 조치할 수 있습니다.

[원클릭 조치]

1. 점검항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. 관리자가 설정한 최근 사용한 패스워드 저장 개수가 사용자 PC에 설정되면 다음과 같은 알림 창이 나타납니다.



3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

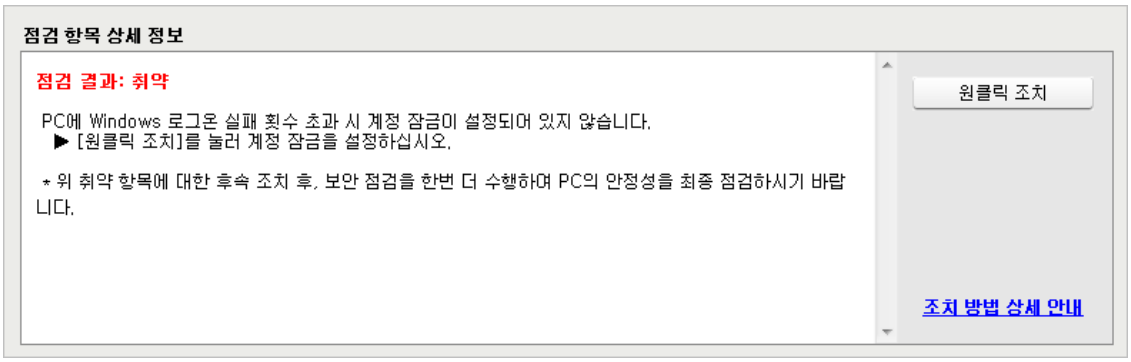
Windows 로그온 실패 횟수 초과 시 계정 잠금 설정 점검

Windows 사용자 계정에 비밀번호를 입력하지 않고 자동으로 로그온 하도록 설정되어 있는지를 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 Windows 로그온 실패 횟수 초과 시 계정이 잠기도록 설정되어 있습니다.
- 취약: PC 에 Windows 로그온 실패 횟수 초과 시 계정을 잠그도록 설정되어 있지 않습니다. **원클릭 조치**를 눌러 계정 잠금을 설정하십시오.

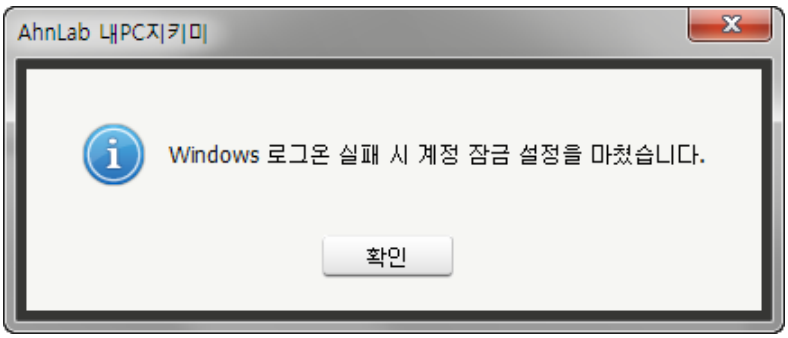


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

1. 점검항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. 원클릭 조치로 Windows 로그온 실패 횟수 초과 시 계정이 잠기도록 설정되면 다음과 같은 알림 창이 나타납니다.

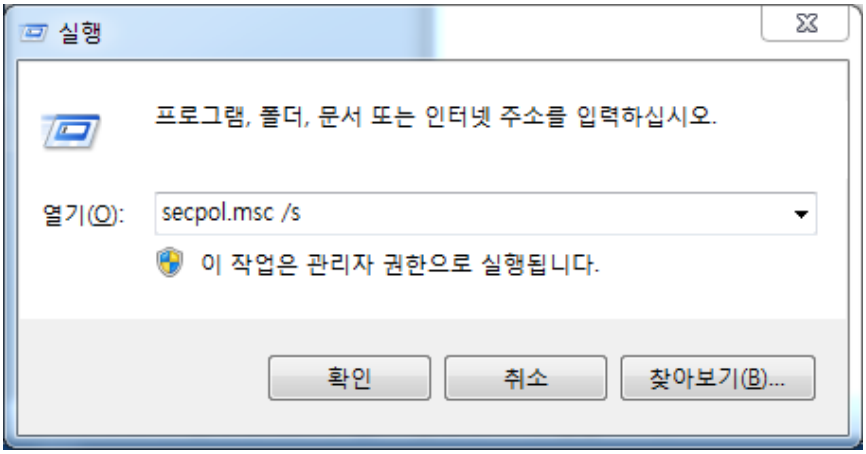


3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

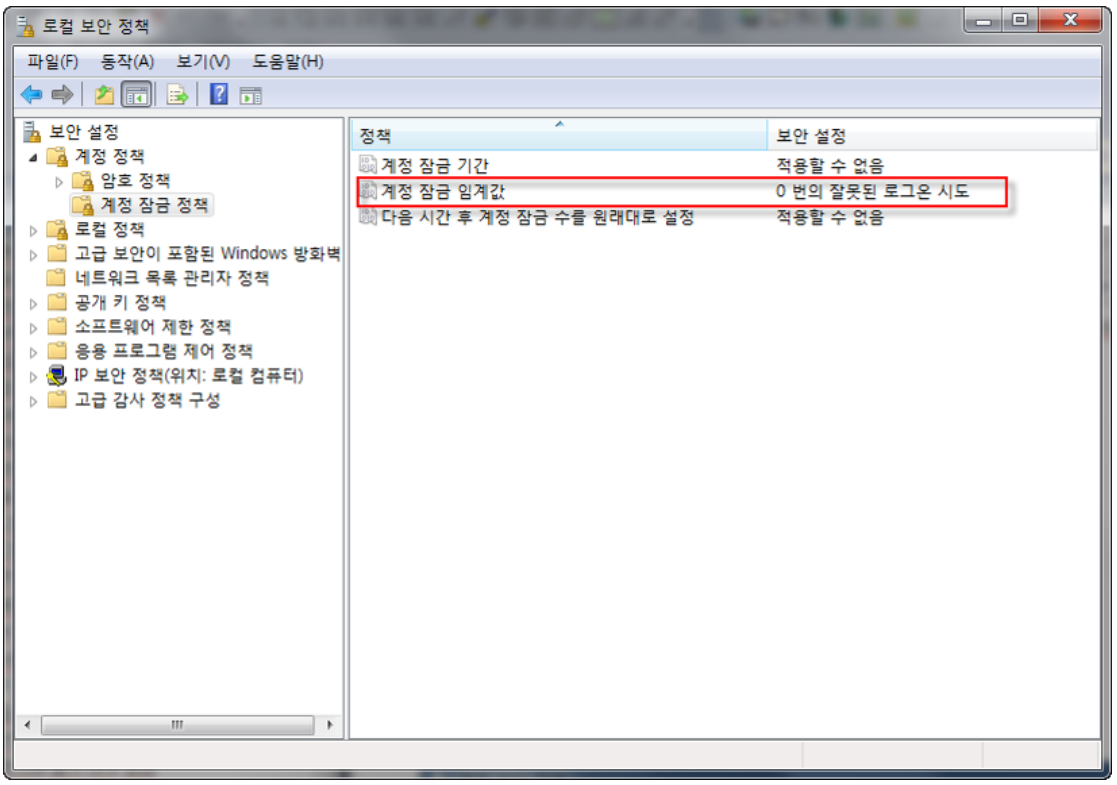
[사용자 조치]

윈도우의 사용자 계정에 자동으로 로그온 하도록 설정된 경우 다음과 같은 방법으로 설정을 해제합니다.

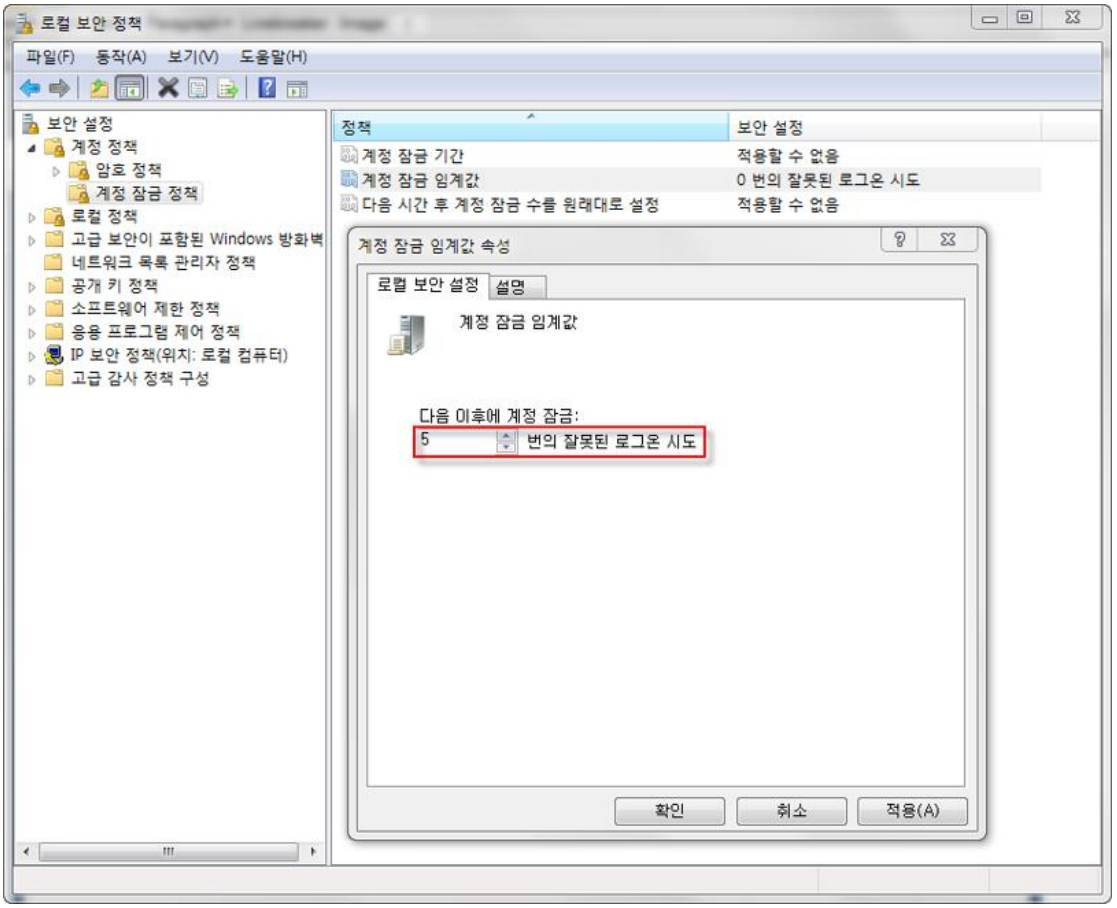
1. 윈도우 + R키를 눌러 실행 창을 띄운 후 **secpol.msc /s**를 입력합니다.



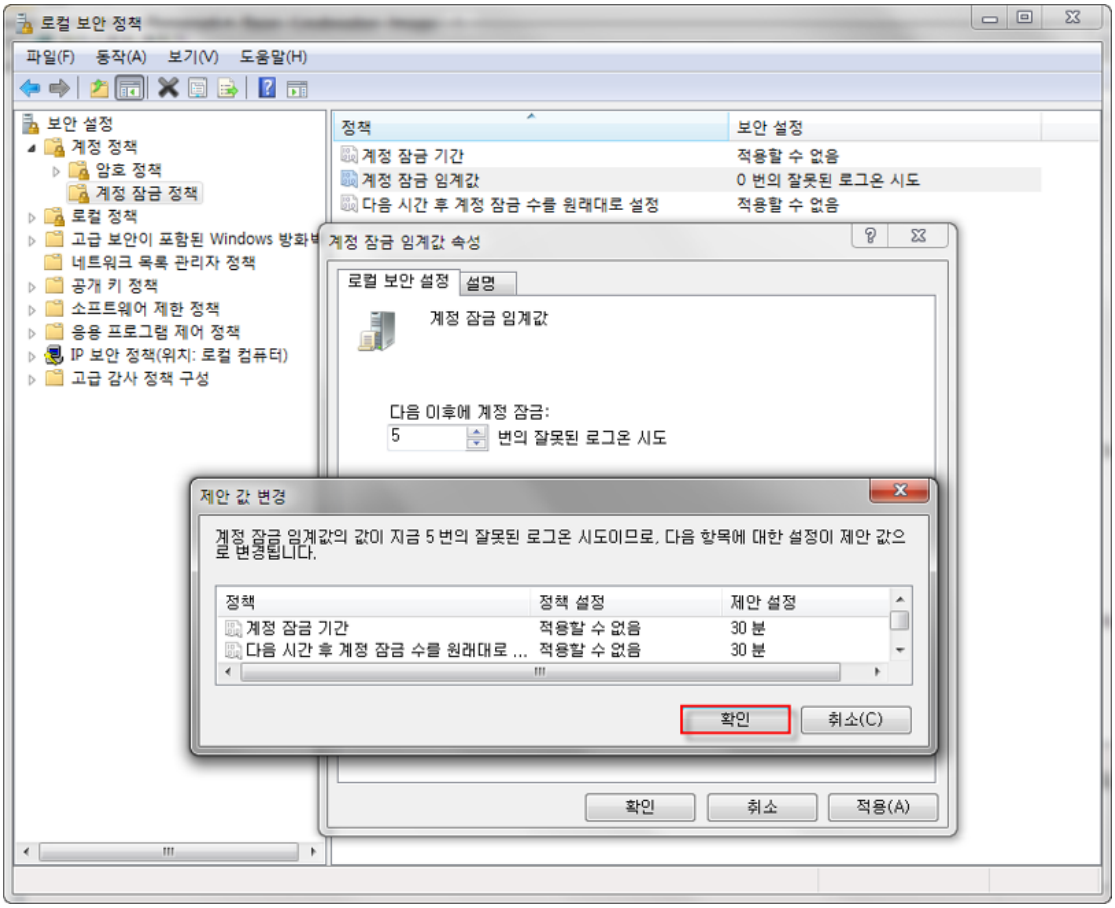
2. **계정 정책**의 하위에 있는 **계정 잠금 정책**에서 **계정 잠금 임계** 값을 더블 클릭합니다.



3. 계정 잠금 임계 값을 0이 아닌 값으로 설정합니다.



4. 계정 잠금 기간과 로그온 실패 횟수의 재설정 기간을 확인 후 **확인**을 클릭하여 설정을 종료합니다.


로컬 보안 정책
파일(F) 동작(A) 보기(V) 도움말(H)
보안 설정
계정 정책
암호 정책
계정 잠금 정책
로컬 정책
고급 보안이 포함된 Windows 방화벽
네트워크 목록 관리자 정책
공개 키 정책
소프트웨어 제한 정책
응용 프로그램 제어 정책
IP 보안 정책(위치: 로컬 컴퓨터)
고급 감사 정책 구성
정책
보안 설정
계정 잠금 기간
적용할 수 없음
계정 잠금 임계값
0 번의 잘못된 로그온 시도
다음 시간 후 계정 잠금 수를 원래대로 설정
적용할 수 없음
계정 잠금 임계값 속성
로컬 보안 설정
설명
계정 잠금 임계값
다음 이후에 계정 잠금:
5
번의 잘못된 로그온 시도
제안 값 변경
계정 잠금 임계값의 값이 지금 5 번의 잘못된 로그온 시도이므로, 다음 항목에 대한 설정이 제안 값으로 변경됩니다.
정책
정책 설정
제안 설정
계정 잠금 기간
적용할 수 없음
30 분
다음 시간 후 계정 잠금 수를 원래대로 ...
적용할 수 없음
30 분
확인
취소(C)
확인
취소
적용(A)

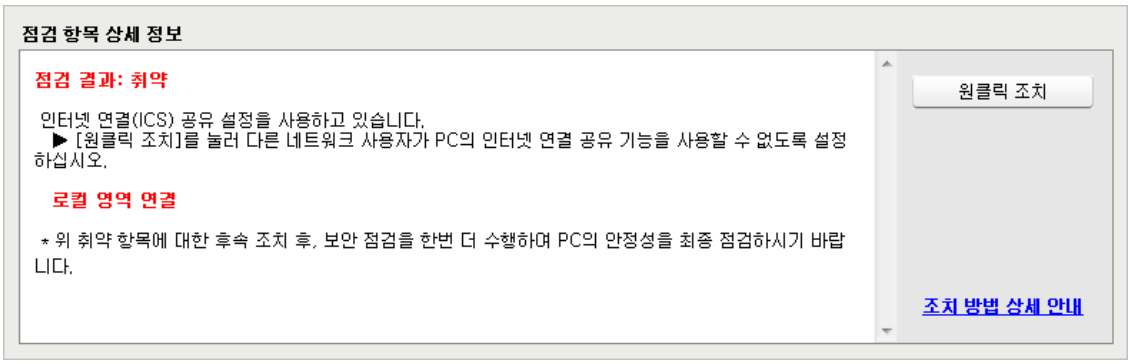
인터넷 연결 공유 사용 점검

다른 네트워크 사용자가 이 컴퓨터의 인터넷 연결 공유 기능을 사용하는 지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: 인터넷 연결 공유를 사용하지 않도록 설정되어 있습니다.
- 취약: 인터넷 연결 공유를 사용하도록 설정되어 있습니다. **원클릭 조치**를 눌러 다른 네트워크 사용자가 PC 의 인터넷 연결 공유 기능을 사용할 수 없도록 설정하십시오.



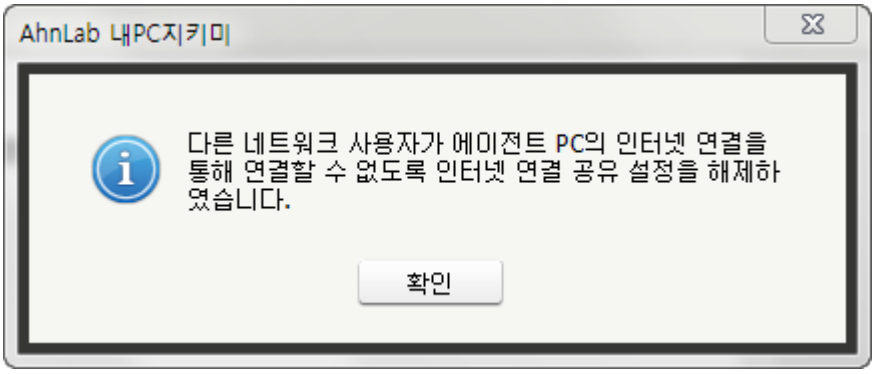
조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

1. 점검항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. 원클릭 조치로 인터넷 연결 공유 설정을 해제하면 다음과 같은 알림 창이 나타납니다.

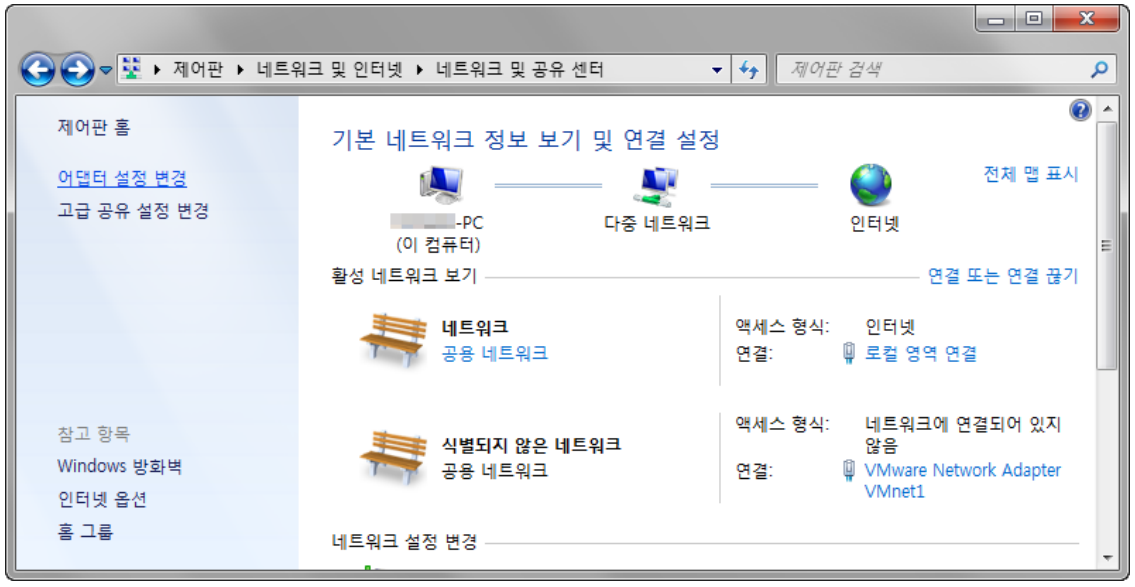


3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

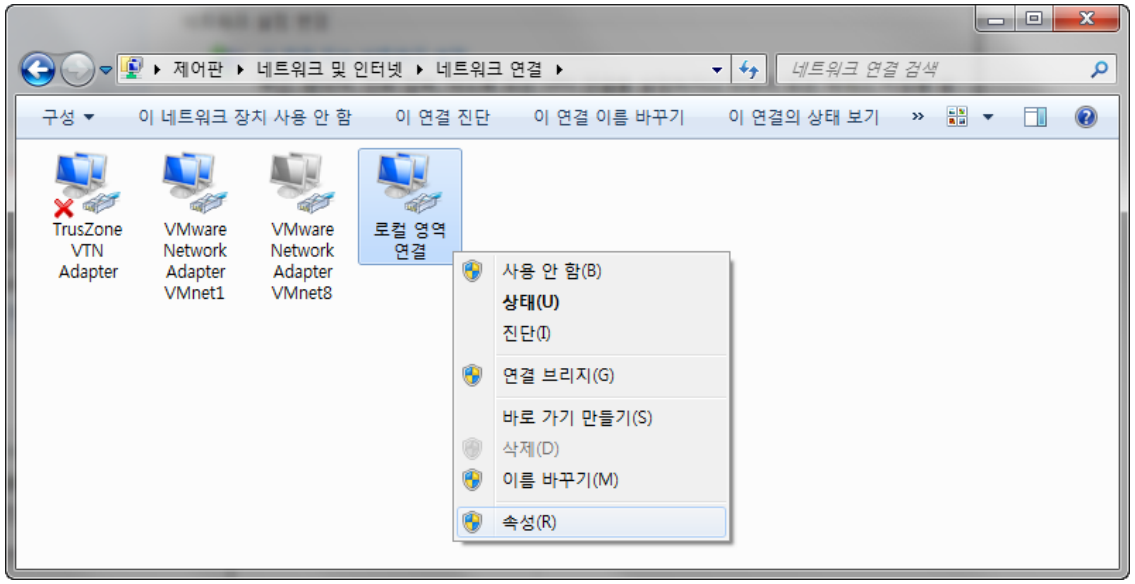
[사용자 조치]

인터넷 연결 공유를 사용하도록 설정된 경우 다음과 같은 방법으로 설정을 해제합니다.

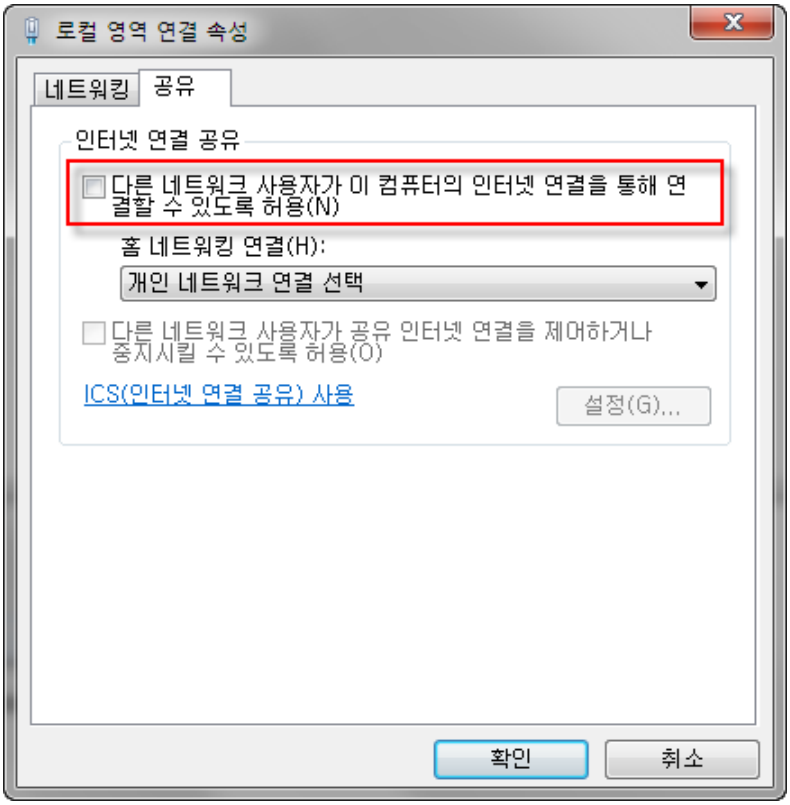
1. 제어판에서 **제어판**> **네트워크 및 인터넷** > **네트워크 및 공유 센터**로 이동합니다.
2. <네트워크 및 공유 센터>에서 **어댑터 설정 변경**을 누릅니다.



3. 로컬 영역 연결 아이콘을 마우스 오른쪽으로 눌러 **속성** 메뉴를 선택합니다.



4. <로컬 영역 연결 속성>의 공유 탭에서 **다른 네트워크 사용자가 이 컴퓨터의 인터넷 연결을 통해 연결할 수 있도록 허용(N)**을 선택 해제합니다.


로컬 영역 연결 속성
네트워킹
공유
인터넷 연결 공유
다른 네트워크 사용자가 이 컴퓨터의 인터넷 연결을 통해 연결할 수 있도록 허용(N)
홈 네트워킹 연결(H):
개인 네트워크 연결 선택
다른 네트워크 사용자가 공유 인터넷 연결을 제어하거나 중지시킬 수 있도록 허용(O)
ICS(인터넷 연결 공유) 사용
설정(G)...
확인
취소

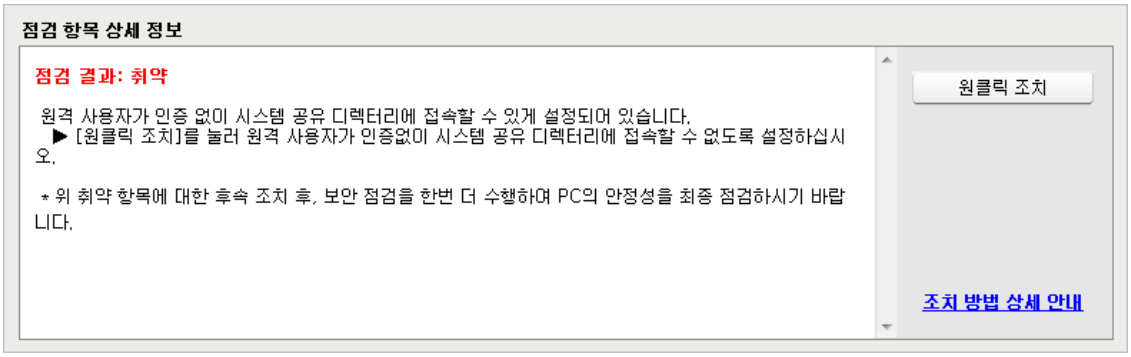
원격 사용자의 시스템 공유 디렉터리 접속 가능 점검

원격에서 사용자 인증 없이 시스템 공유 디렉터리에 접속할 때, 차단 하도록 설정되었는 지를 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: 원격 사용자가 시스템 공유 디렉터리에 접속할 때 인증 여부를 확인하도록 설정되어 있습니다.
- 취약: 원격 사용자가 인증 없이 시스템 공유 디렉터리에 접속할 수 있게 설정되어 있습니다. **원클릭 조치**를 눌러 원격 사용자가 인증 없이 시스템 공유 디렉터리에 접속할 수 없도록 설정하십시오.

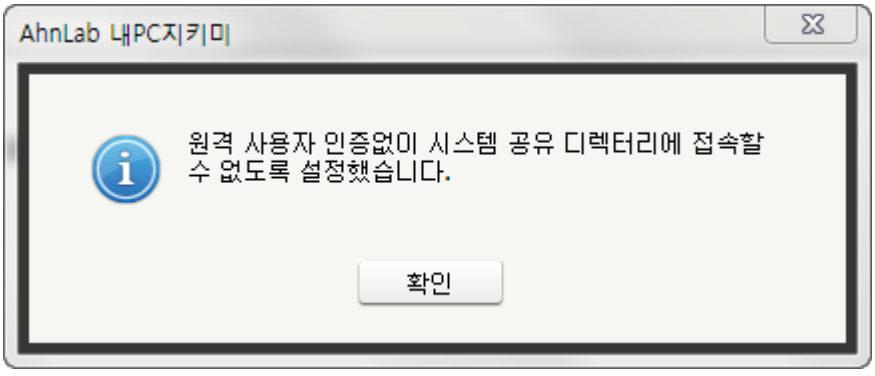


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

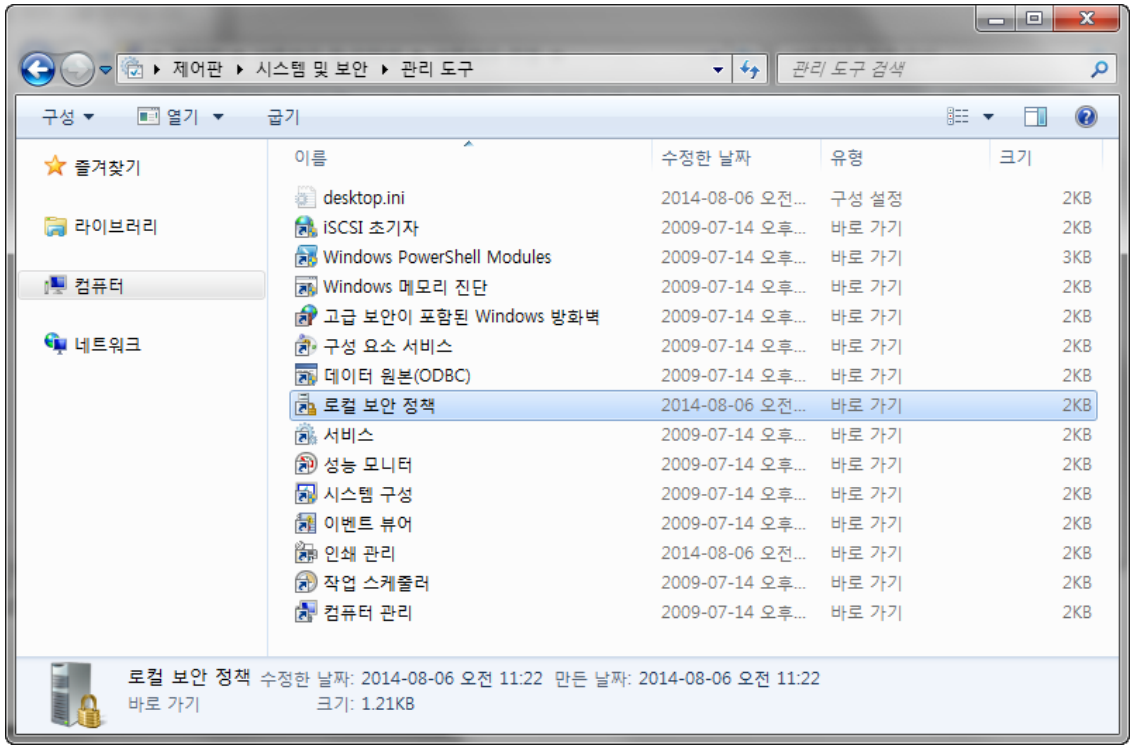
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 원격 사용자 인증 없이 시스템 공유 디렉터리에 접속할 수 없도록 설정하면 다음과 같은 알림 창이 나타납니다.



3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

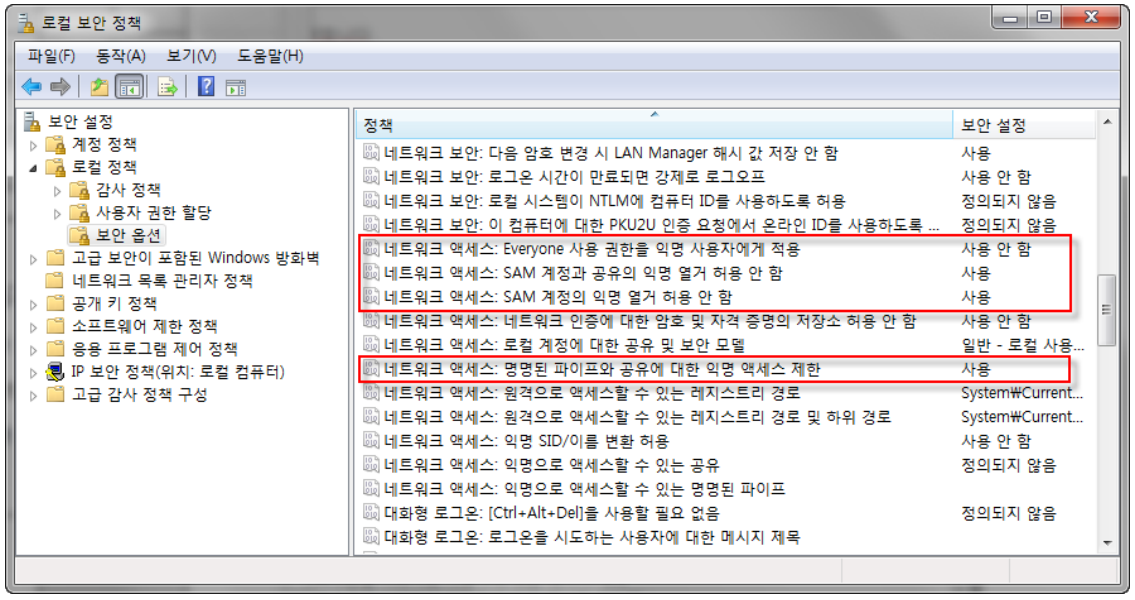
[사용자 조치]

1. 제어판에서 **제어판** > **시스템 및 보안** > **관리 도구**로 이동합니다.
2. <관리 도구>에서 **로컬 보안 정책**을 누릅니다.

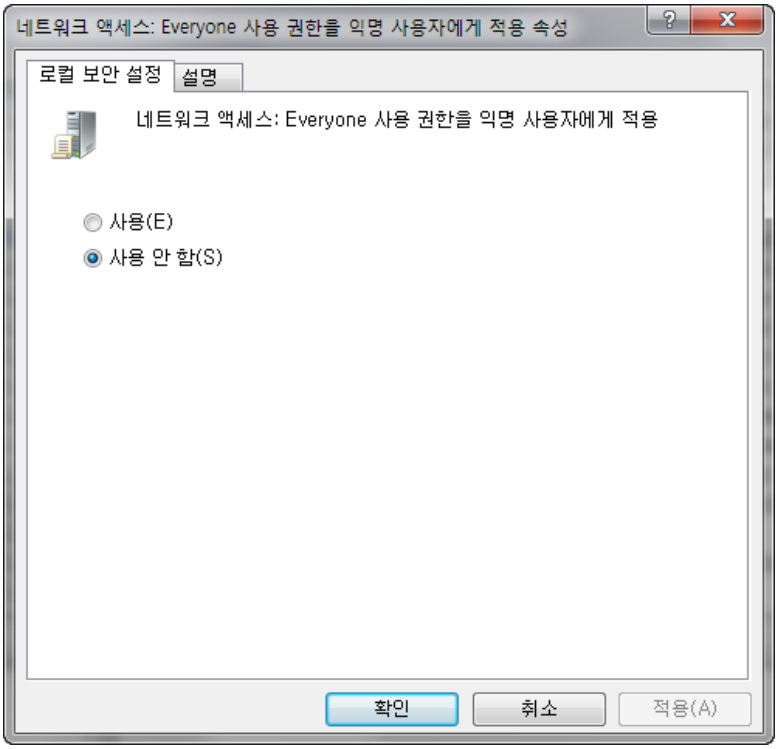


3. <로컬 보안 정책>의 왼쪽 트리에서 로컬 정책의 **보안 옵션**을 선택합니다.

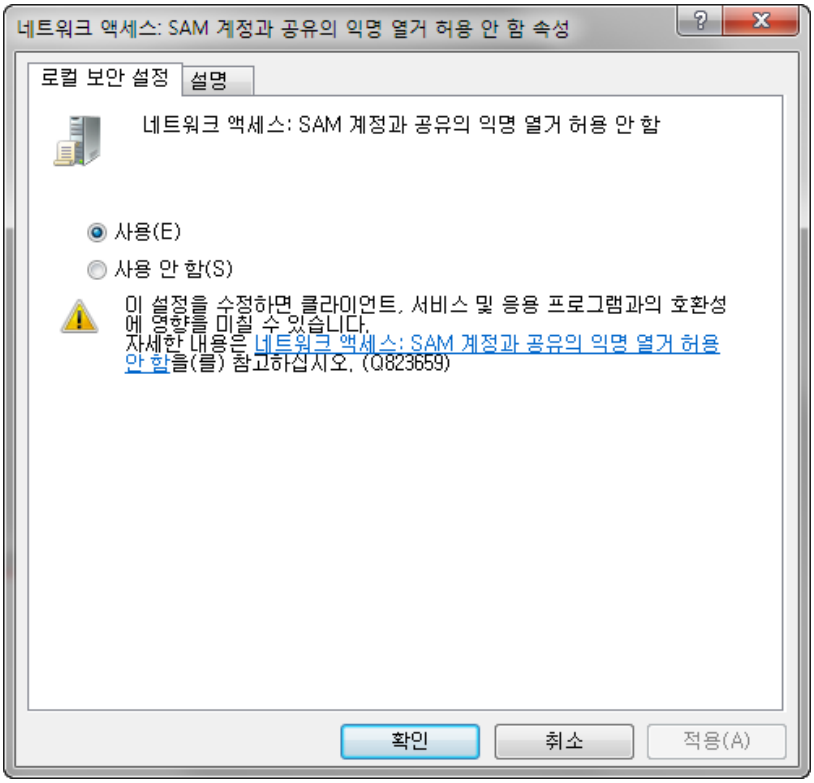
4. 오른쪽 화면에서 아래 정책 설정 값들의 보안 설정을 변경합니다.



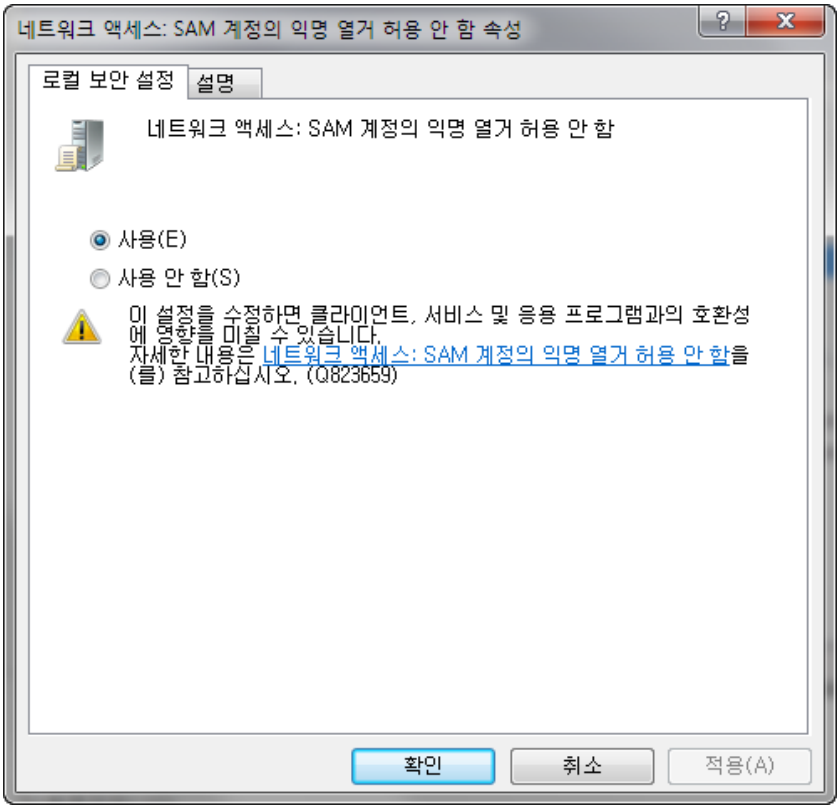
- **네트워크 액세스: Everyone 사용 권한을 익명 사용자에게 적용**을 더블 클릭하여 로컬 보안 설정 탭에서 **사용 안 함(S)**을 선택합니다.



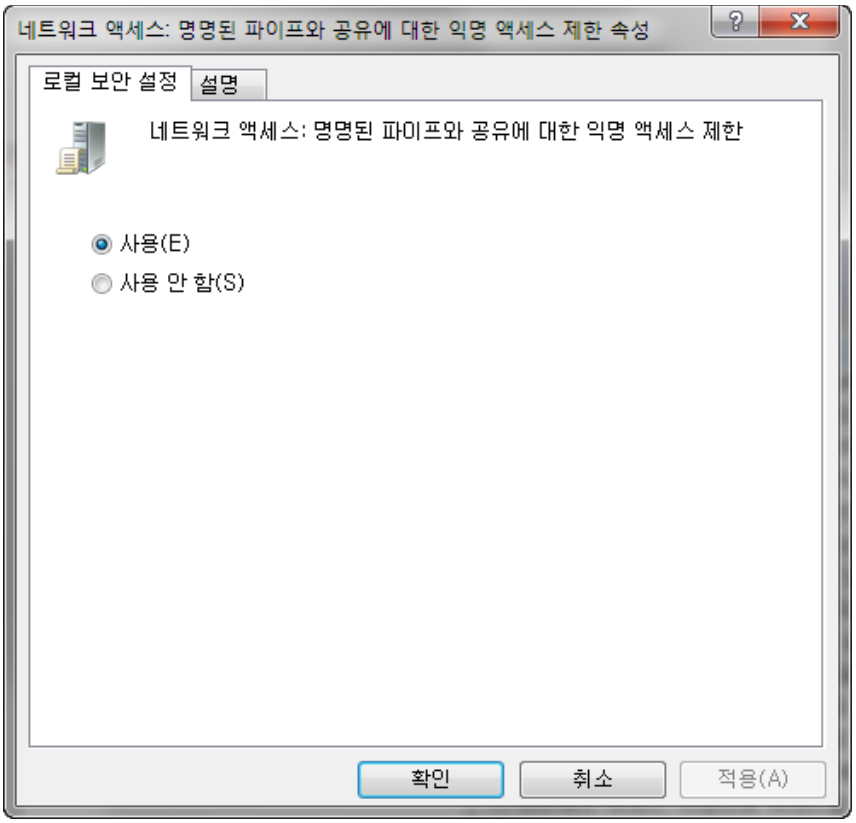
- **네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함**을 더블 클릭하여 로컬 보안 설정 탭에서 **사용(E)**을 선택합니다.



- **네트워크 액세스: SAM 계정의 익명 열거 허용 안 함**을 더블 클릭하여 로컬 보안 설정 탭에서 **사용(E)**을 선택합니다.



- **네트워크 액세스: 명명된 파이프와 공유에 대한 익명 액세스 제한**을 더블 클릭하여 로컬 보안 설정 탭에서 **사용(E)**을 선택합니다.



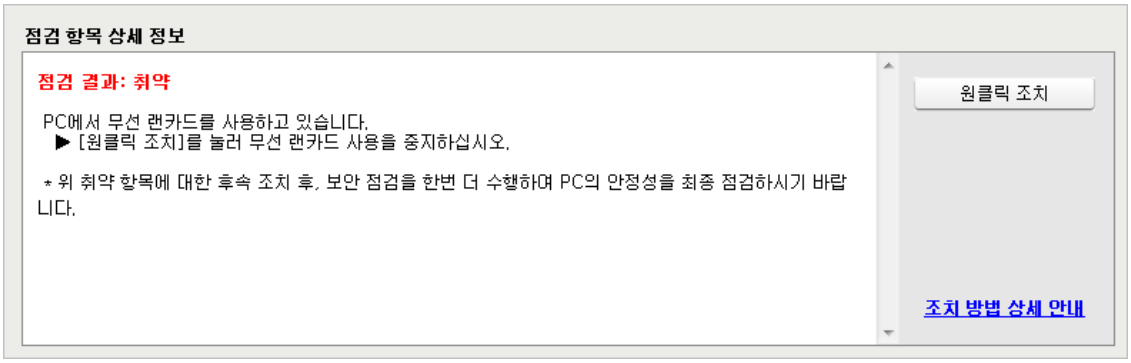
무선 랜카드 사용 점검

사용자 PC 에서 무선 랜카드를 사용 중인지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에서 무선 랜카드를 사용하지 않습니다.
- 취약: PC 에서 무선 랜카드를 사용하고 있습니다. **원클릭 조치**를 눌러 무선 랜카드 사용을 중지하십시오.

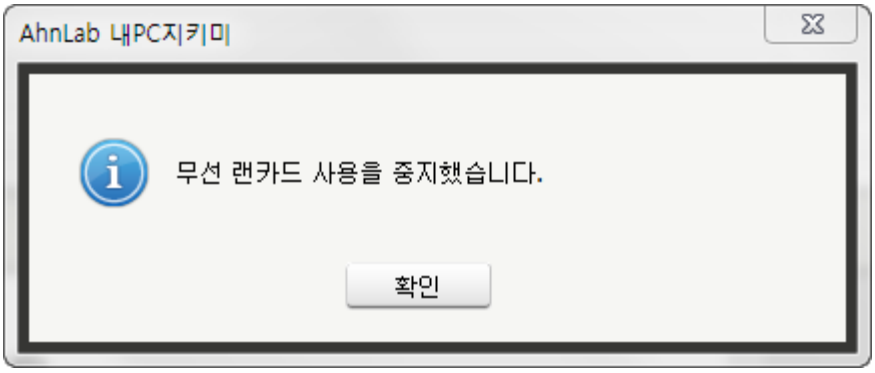


조치 방법

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 PC 에 사용 중인 무선 랜카드를 모두 사용 중지하도록 설정하면 다음과 같은 알림 창이 나타납니다.



3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

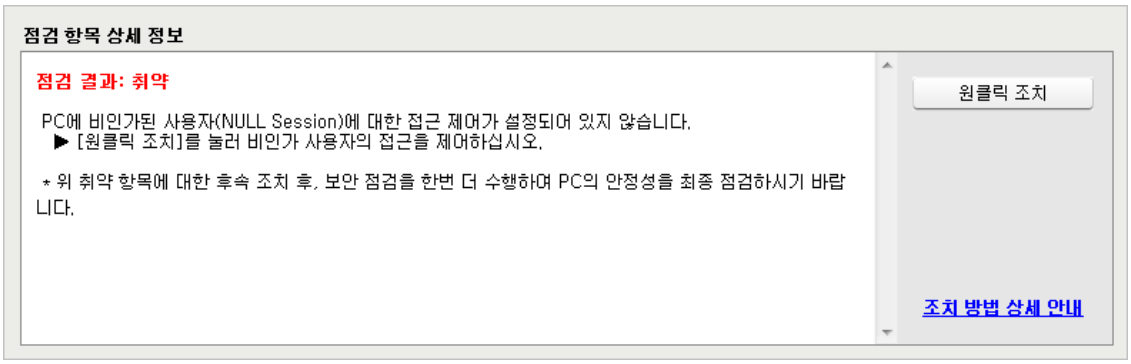
비인가 사용자 접근 제어(NULL Session 접근 제어) 점검

사용자 PC 에 비인가된 사용자 접근 제어가 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 비인가된 사용자(NULL Session)의 접근 제어가 설정되어 있습니다.
- 취약: PC 에 비인가된 사용자(NULL Session)의 접근을 허용하도록 설정되어 있습니다. **원클릭 조치**를 눌러 비인가 사용자에 대한 접근을 허용하지 않도록 설정하십시오.

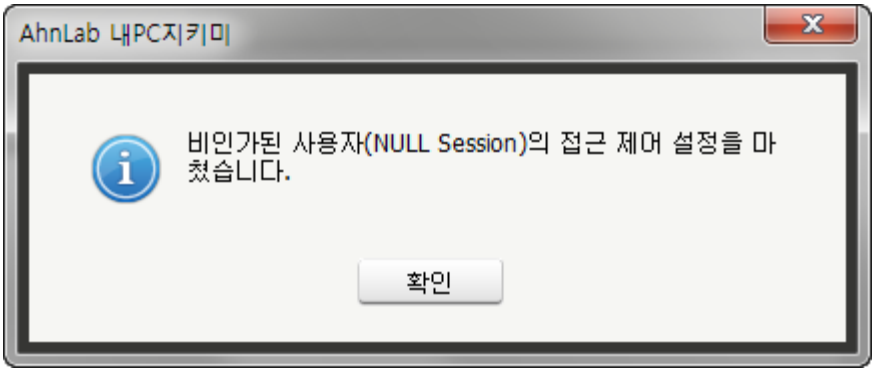


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 비인가 사용자에 대한 접근 제거 설정을 완료하면 다음과 같은 알림 창이 나타납니다.

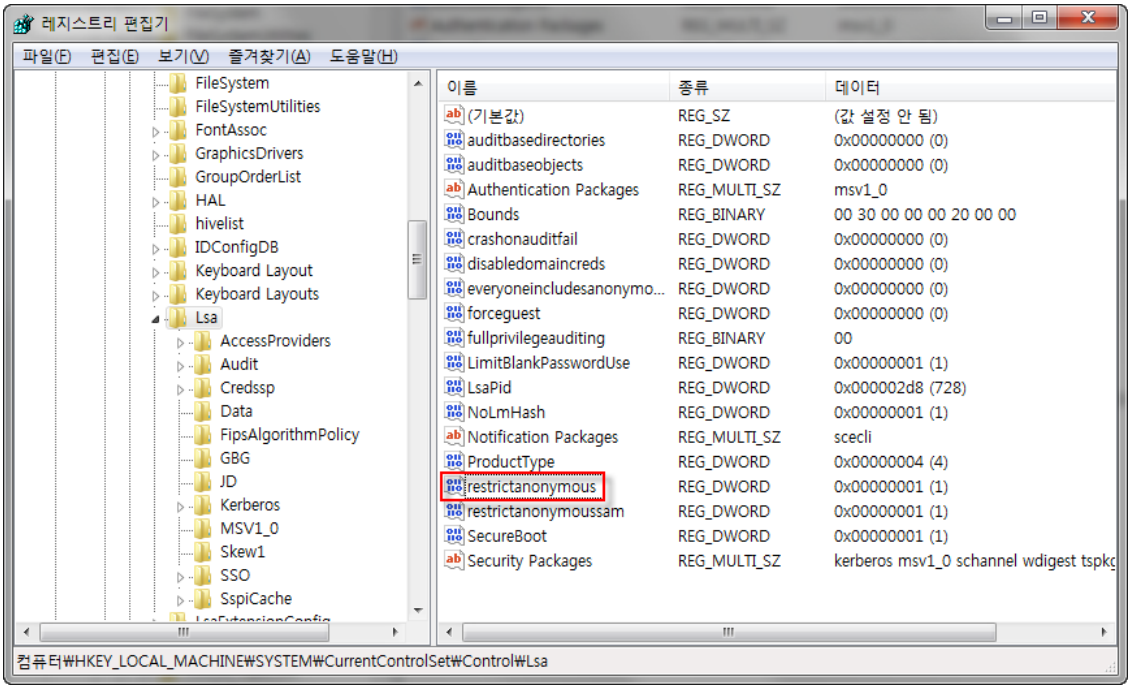


3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

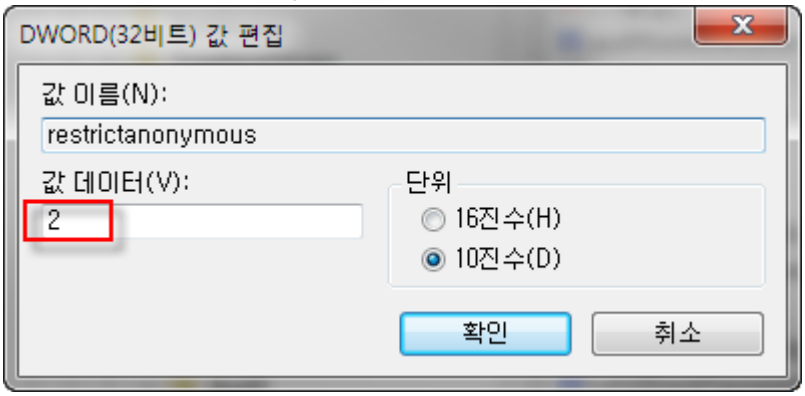
[사용자 조치]

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

1. 레지스트리를 통해 자신의 시스템 환경에 맞게 **restrictanonymous** 값을 적절히 설정합니다.
   Restrictanonymous = 0 로 설정 하면 취약이 되며, 이외의 값은 안전으로 표시 합니다. (Windows2000 계열 이전 버전의 윈도우와 연결 상의 문제가 발생할 수 있습니다.)



2. 다음과 같이 restrictanonymous 값의 데이터를 0 이외의 값으로 변경합니다.



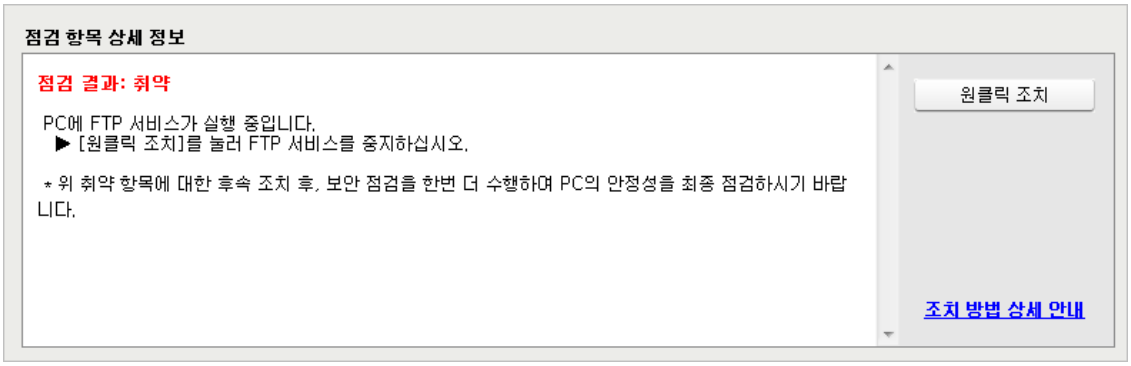
FTP 서비스 실행 점검

사용자 PC 에서 FTP 서버를 사용 중인지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 실행 중인 FTP 서비스가 없습니다.
- 취약: PC 에 FTP 서비스가 실행 중입니다. **원클릭 조치**를 눌러 FTP 서비스를 중지하십시오.

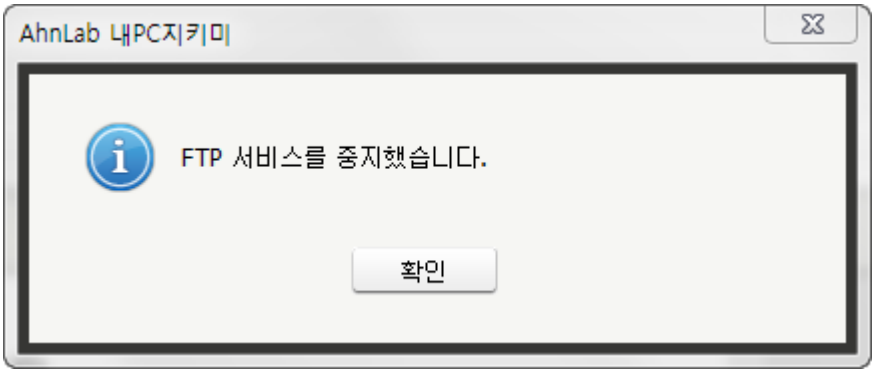


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. FTP 서비스가 중지되고 다음과 같은 알림 창이 발생합니다.

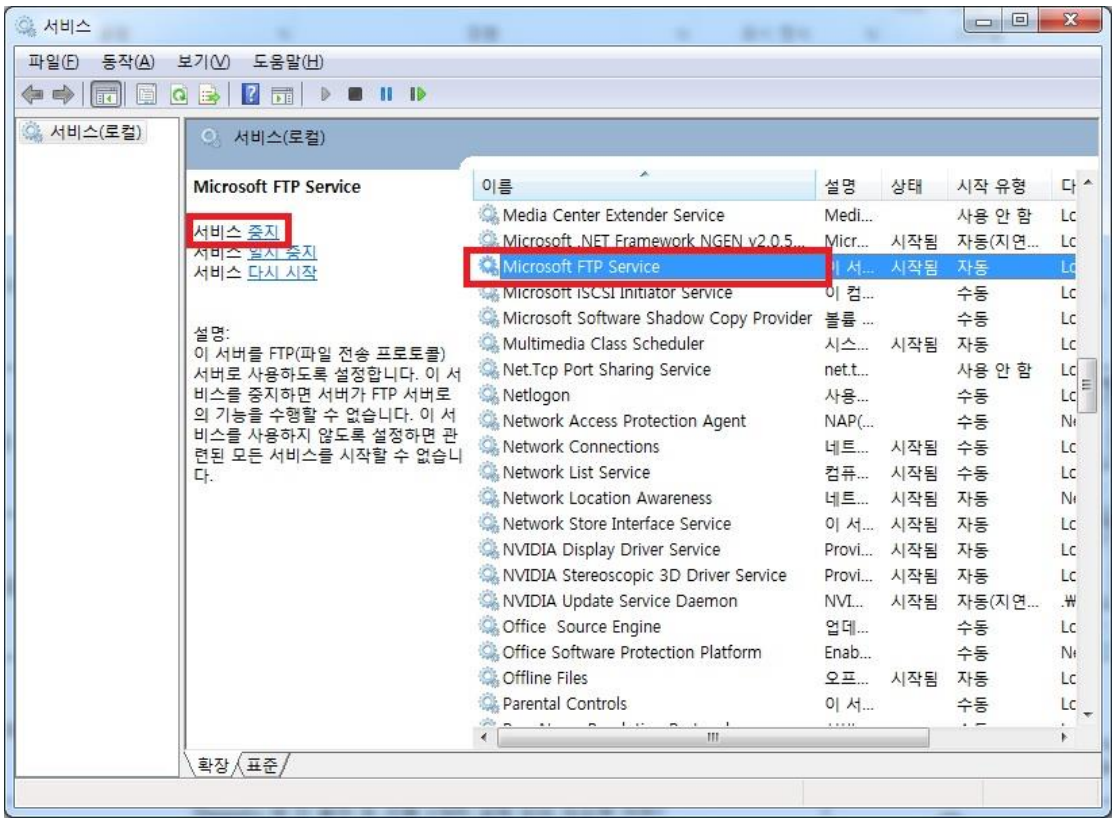


3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. Windows **작업 표시줄의 시작** > **설정** > **제어판** > **시스템 및 보안** > **관리 도구**를 선택한 후 **서비스**를 더블 클릭하여 실행합니다.
2. 서비스 목록에서 **Microsoft FTP Service** 를 선택합니다.

3. **서비스 중지**를 클릭하여 **Microsoft FTP Service** 서비스를 중지합니다.



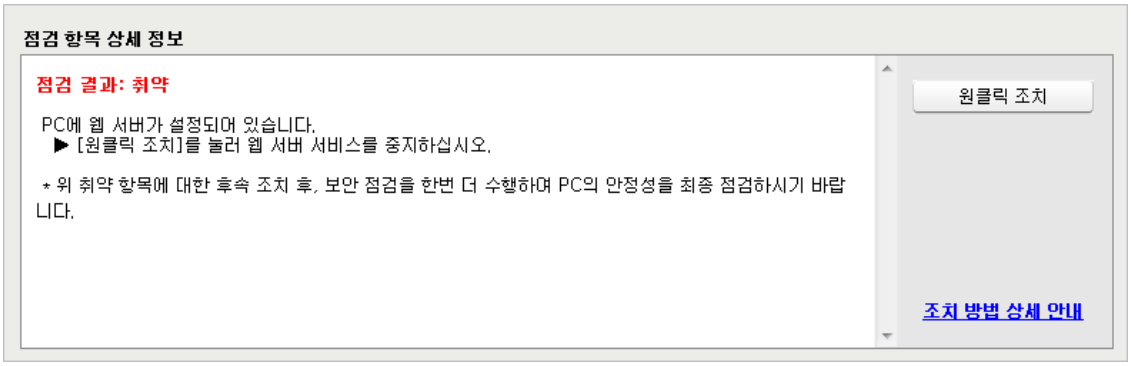
웹 서비스 실행 점검

사용자 PC 에서 웹 서비스가 사용 중인지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 실행 중인 웹 서비스가 없습니다.
- 취약: PC 에 웹 서비스가 실행 중입니다. **원클릭 조치**를 눌러 웹 서비스를 중지하십시오.

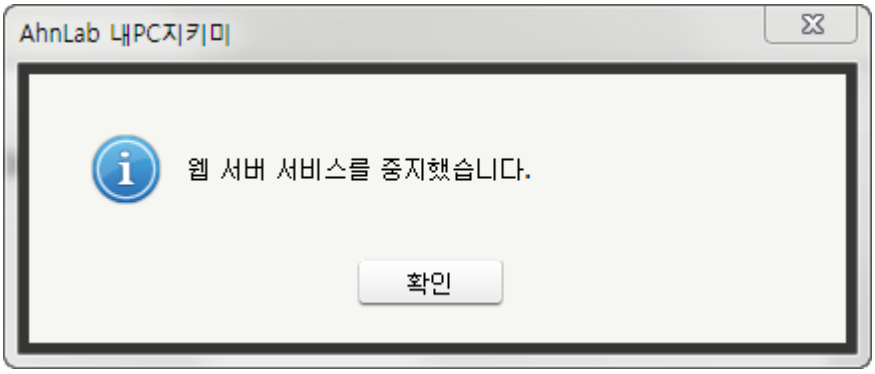


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

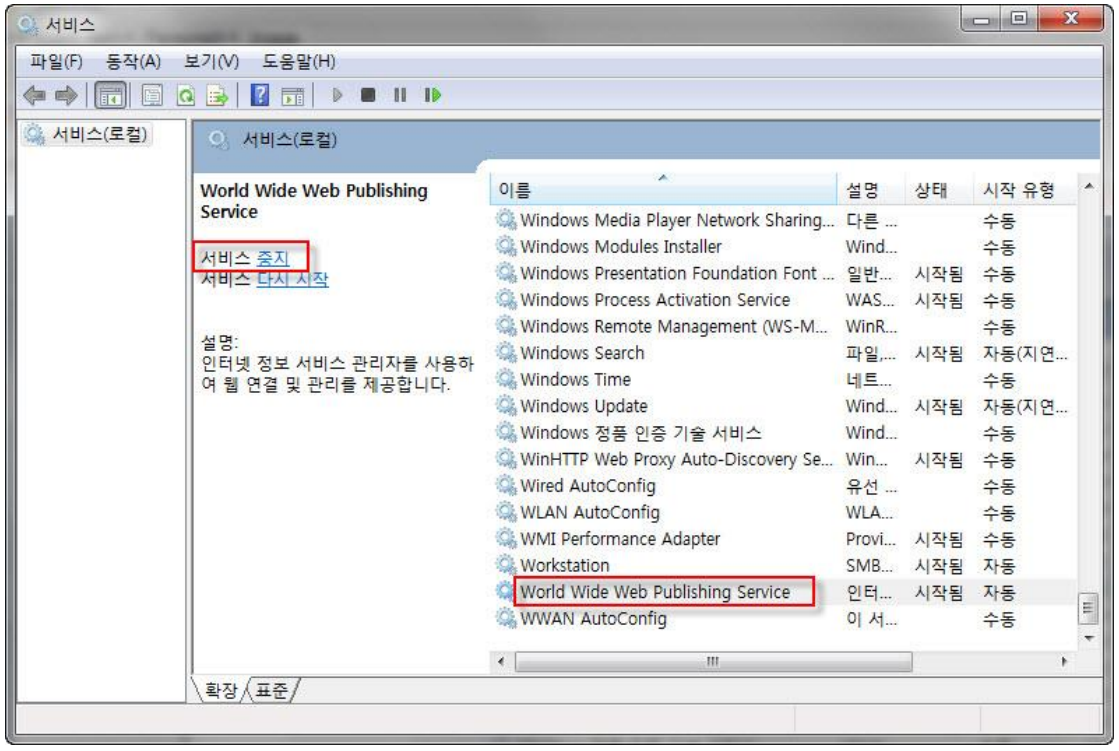
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. World Wide Web Publishing Service 서비스가 중지되고 다음과 같은 알림 창이 발생합니다.



3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. Windows 작업 표시줄의 **시작** > **설정** > **제어판** > **시스템 및 보안** > **관리 도구**를 선택한 후, **서비스**를 더블 클릭하여 실행합니다.
2. 서비스 목록에서 **World Wide Web Publishing Service**를 선택합니다.
3. 서비스 중지를 눌러 **World Wide Web Publishing Service** 서비스를 중지합니다.


서비스
파일(F) 동작(A) 보기(V) 도움말(H)
서비스(로컬)
서비스(로컬)
World Wide Web Publishing Service
서비스 중지
서비스 다시 시작
설명:
인터넷 정보 서비스 관리자를 사용하여 웹 연결 및 관리를 제공합니다.
이름 설명 상태 시작 유형
Windows Media Player Network Sharing... 다른 ... 수동
Windows Modules Installer Wind... 수동
Windows Presentation Foundation Font ... 일반... 시작됨 수동
Windows Process Activation Service WAS... 시작됨 수동
Windows Remote Management (WS-M... WinR... 수동
Windows Search 파일,... 시작됨 자동(지연...
Windows Time 네트... 수동
Windows Update Wind... 시작됨 자동(지연...
Windows 정품 인증 기술 서비스 Wind... 수동
WinHTTP Web Proxy Auto-Discovery Se... Win... 시작됨 수동
Wired AutoConfig 유선 ... 수동
WLAN AutoConfig WLA... 수동
WMI Performance Adapter Provi... 시작됨 수동
Workstation SMB... 시작됨 자동
World Wide Web Publishing Service 인터... 시작됨 자동
WWAN AutoConfig 이 서... 수동
확장 표준

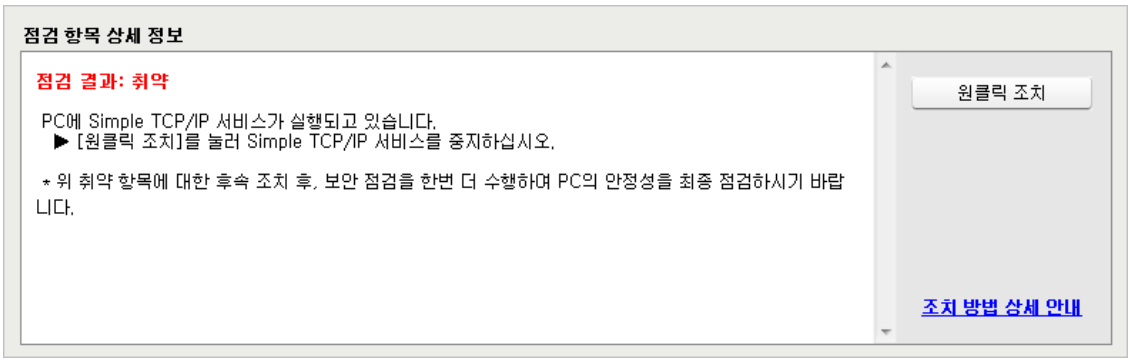
Simple TCP/IP 서비스 실행 점검

사용자 PC 에서 Simple TCP/IP 서비스가 실행 중인지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 실행 중인 Simple TCP/IP 서비스가 없습니다.
- 취약: PC 에 Simple TCP/IP 서비스가 실행되고 있습니다. **원클릭 조치**를 눌러 Simple TCP/IP 서비스를 중지하십시오.

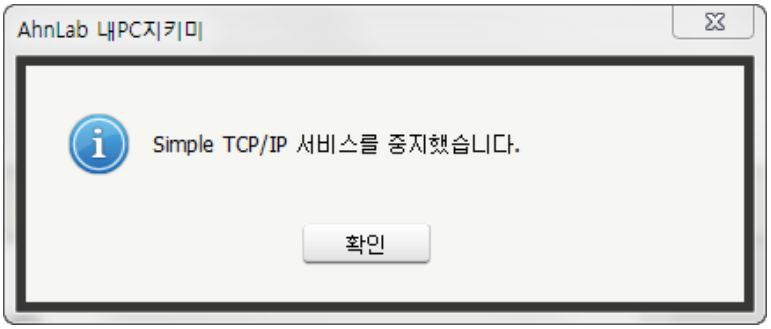


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

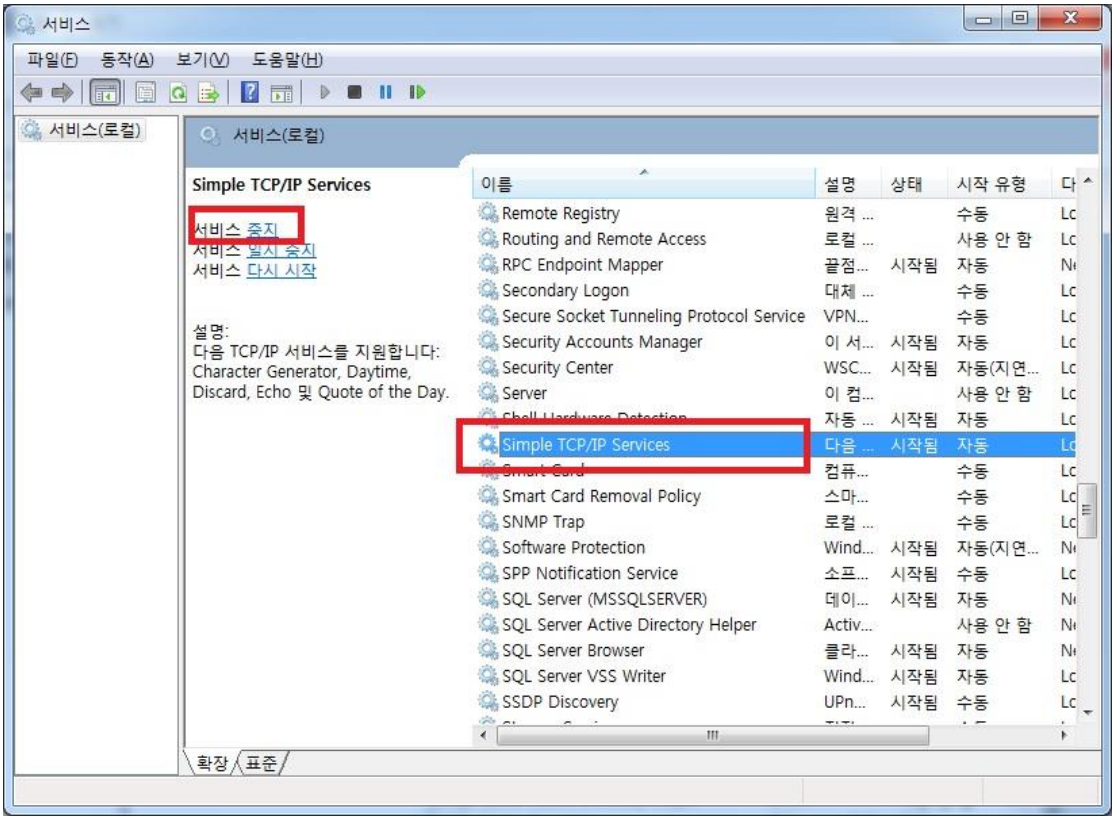
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. Simple TCP/IP 서비스가 중지되고 다음과 같은 알림 창이 발생합니다.



3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. Windows 작업 표시줄의 **시작** > **설정** > **제어판** > **시스템 및 보안** > **관리 도구**를 선택한 후 **서비스**를 더블 클릭하여 실행합니다.
2. **Simple TCP/IP Services** 서비스를 **중지**합니다.


서비스
파일(F) 동작(A) 보기(V) 도움말(H)
서비스(로컬)
서비스(로컬)
Simple TCP/IP Services
서비스 중지
서비스 일시 중지
서비스 다시 시작
설명:
다음 TCP/IP 서비스를 지원합니다:
Character Generator, Daytime,
Discard, Echo 및 Quote of the Day.
이름 설명 상태 시작 유형
Remote Registry 원격 ... 수동
Routing and Remote Access 로컬 ... 사용 안 함
RPC Endpoint Mapper 끝점... 시작됨 자동
Secondary Logon 대체 ... 수동
Secure Socket Tunneling Protocol Service VPN... 수동
Security Accounts Manager 이 서... 시작됨 자동
Security Center WSC... 시작됨 자동(지연...
Server 이 컴... 사용 안 함
자동 ... 시작됨 자동
Simple TCP/IP Services 다음 ... 시작됨 자동
컴퓨... 수동
Smart Card Removal Policy 스마... 수동
SNMP Trap 로컬 ... 수동
Software Protection Wind... 시작됨 자동(지연...
SPP Notification Service 소프... 시작됨 수동
SQL Server (MSSQLSERVER) 데이... 시작됨 자동
SQL Server Active Directory Helper Activ... 사용 안 함
SQL Server Browser 클라... 시작됨 자동
SQL Server VSS Writer Wind... 시작됨 자동
SSDP Discovery UPn... 시작됨 수동
확장 표준

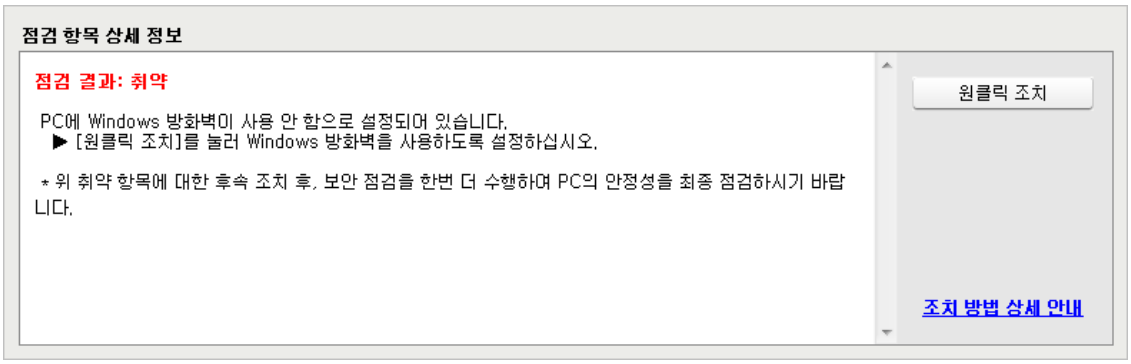
Windows 방화벽 사용 점검

사용자 PC 에 Windows 방화벽이 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 Windows 방화벽을 사용하고 있습니다.
- 취약: PC 에 Windows 방화벽이 사용 안 함으로 설정되어 있습니다. **원클릭 조치**를 눌러 Windows 방화벽을 사용하도록 설정하십시오.

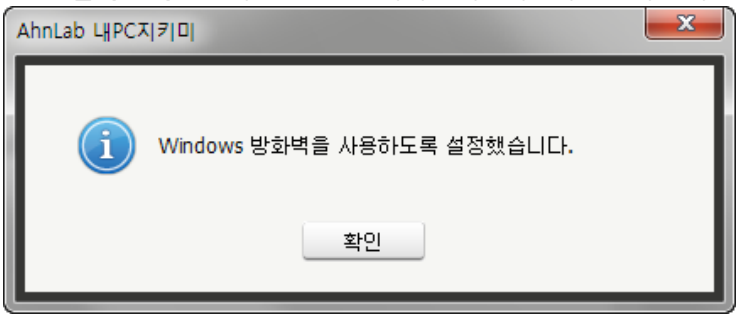


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

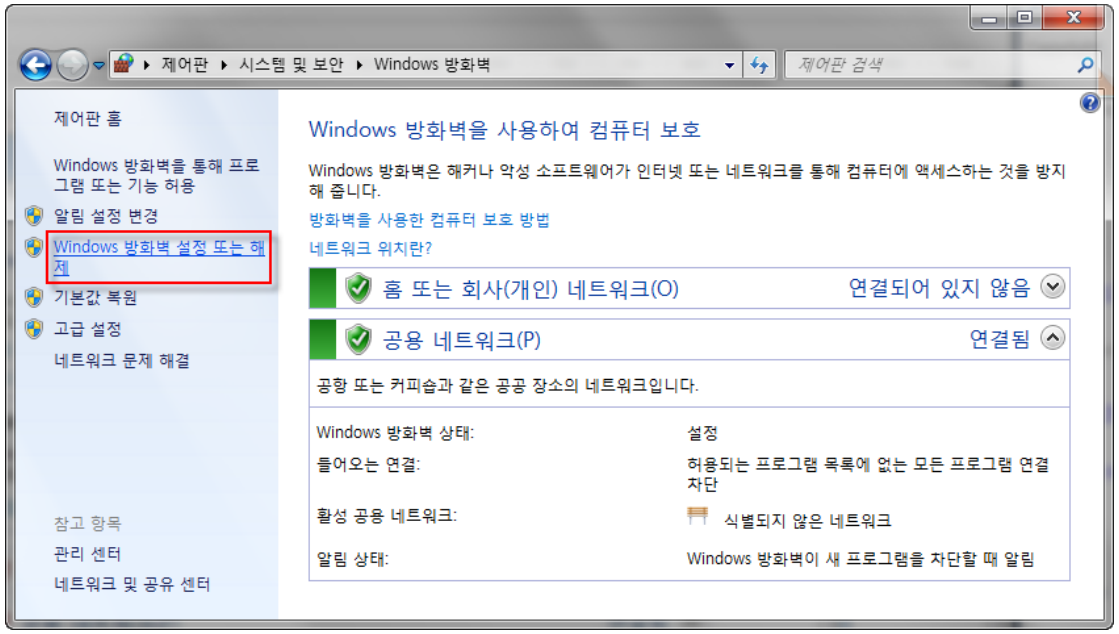
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 Windows 방화벽을 사용하도록 설정하면 다음과 같은 알림 창이 나타납니다.



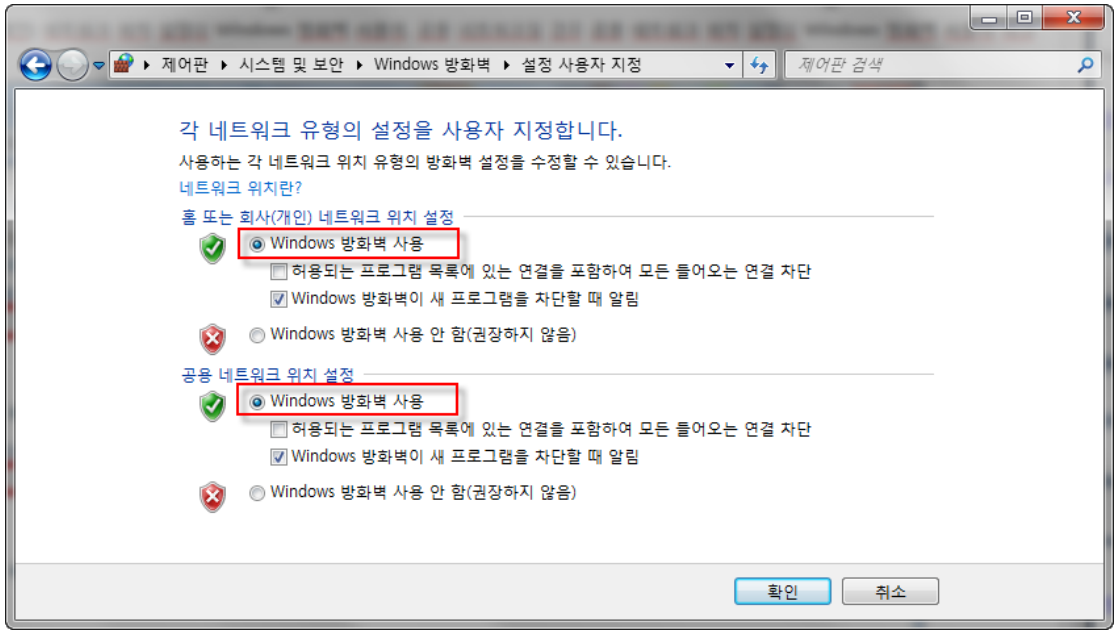
3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. Windows 작업 표시줄의 **시작** > **설정** > **제어판** > **시스템 및 보안** > **Windows 방화벽**을 선택한 후 **Windows 방화벽 설정 또는 해제**를 선택합니다.



2. 개인 네트워크일 경우 **홈 또는 회사(개인) 네트워크 위치 설정**의 **Windows 방화벽 사용**에, 공용 네트워크일 경우 **공용 네트워크 위치 설정**의 **Windows 방화벽 사용**에 체크 후 **확인**을 눌러 저장합니다.



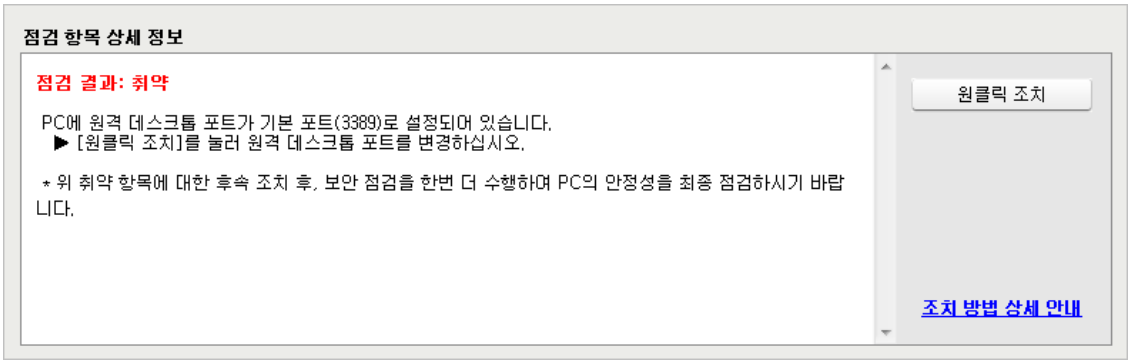
원격 데스크톱 포트 변경 점검

사용자 PC 의 원격 데스크톱 포트가 변경되었는지 점검합니다. 원격 데스크톱은 기본적으로 3389 포트를 사용합니다. 아래 조치 방법과 같이 기본 포트를 변경해야 합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 의 원격 데스크톱 포트가 기본 포트(3389)가 아닌 변경된 포트로 설정되어 있습니다.
- 취약: PC 에 원격 데스크톱 포트가 기본 포트(3389)로 설정되어 있습니다. **원클릭 조치**를 눌러 원격 데스크톱 포트를 변경하십시오.

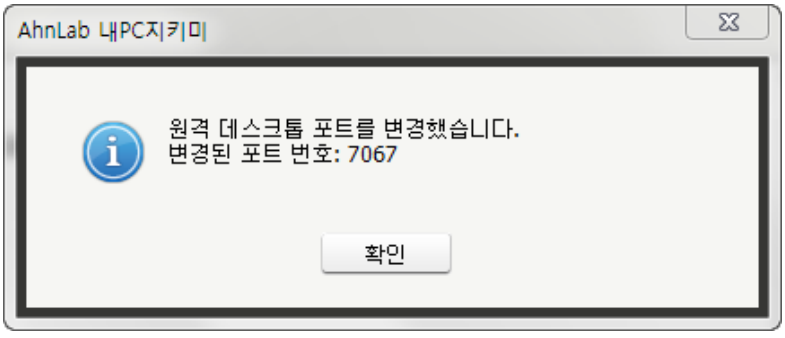


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 누르면 원격 데스크톱 포트가 기본 포트(3389)에서 변경되며, 다음과 같은 알림 창이 나타납니다.

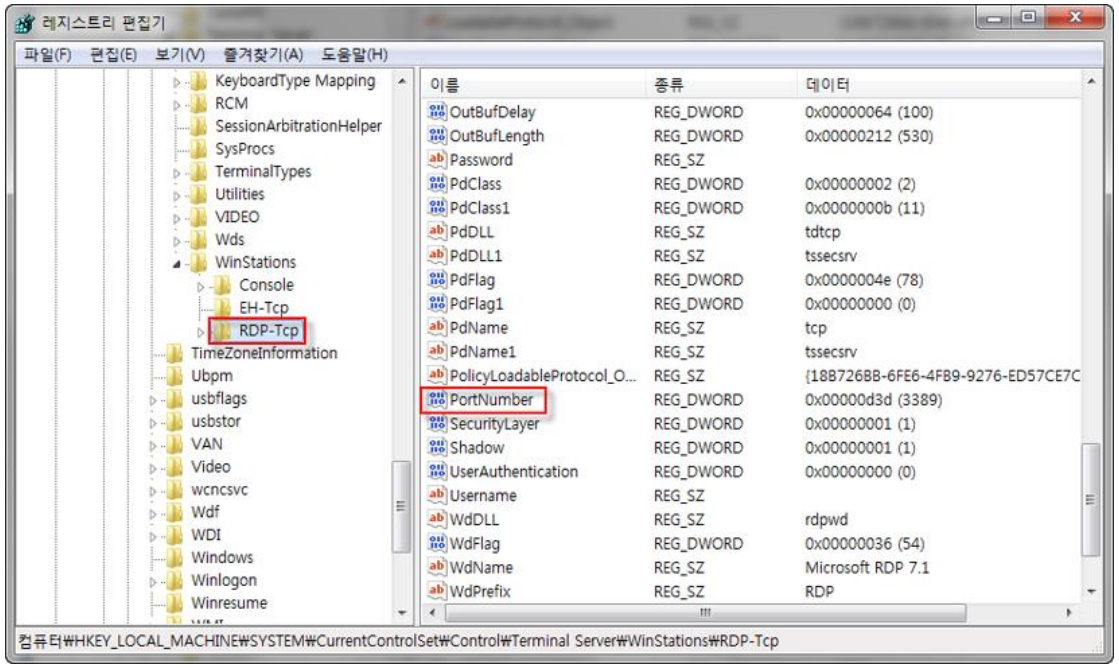


3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

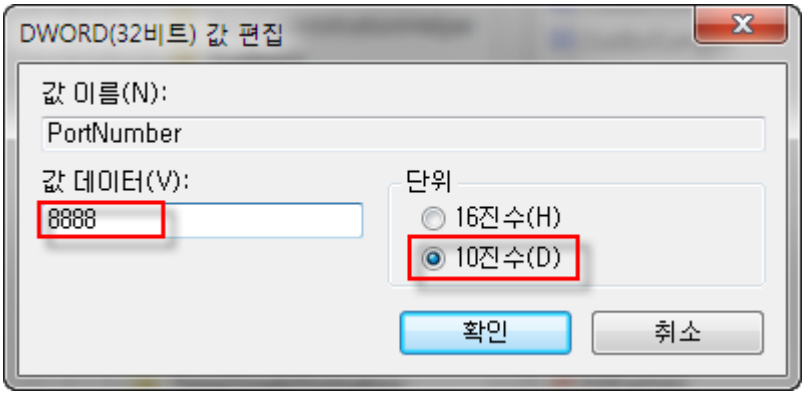
[사용자 조치]

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

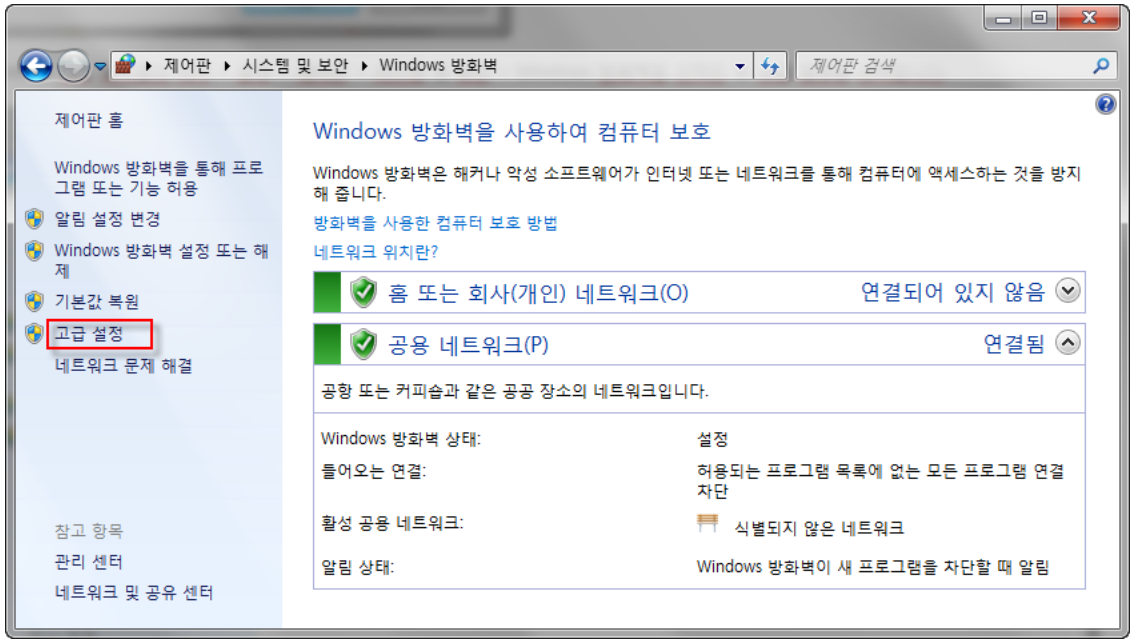
1. 레지스트리 편집기를 열고 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp**의 **PortNumber**를 더블 클릭하여 엽니다.



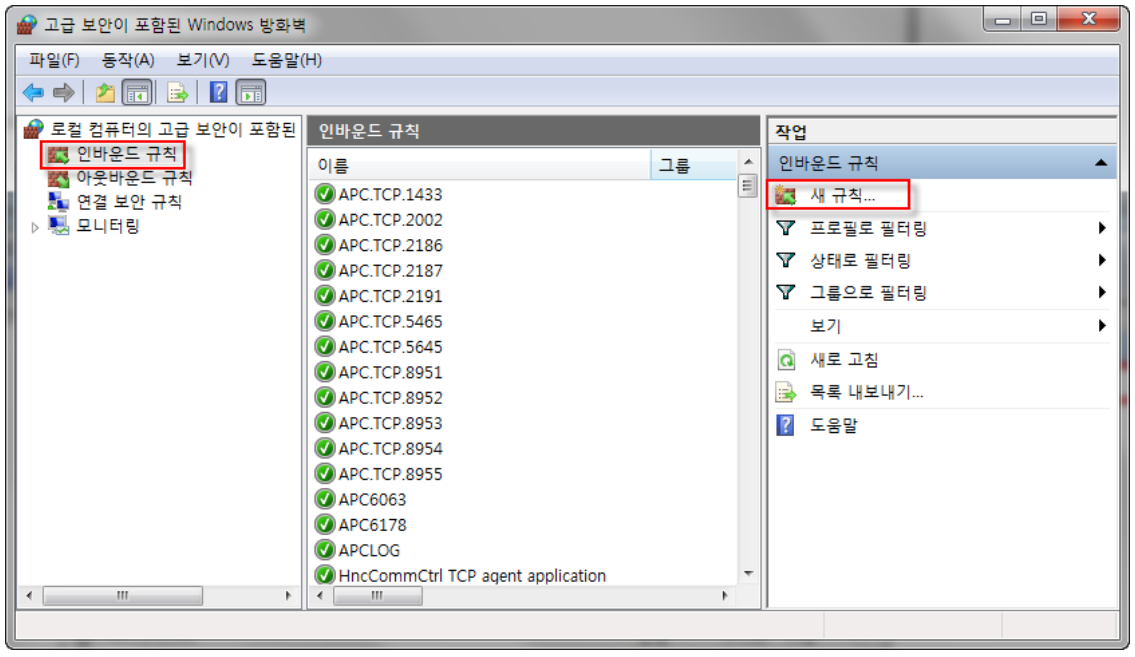
2. **10진수**에 체크하고 변경할 포트 번호를 넣고 **확인**을 누릅니다.



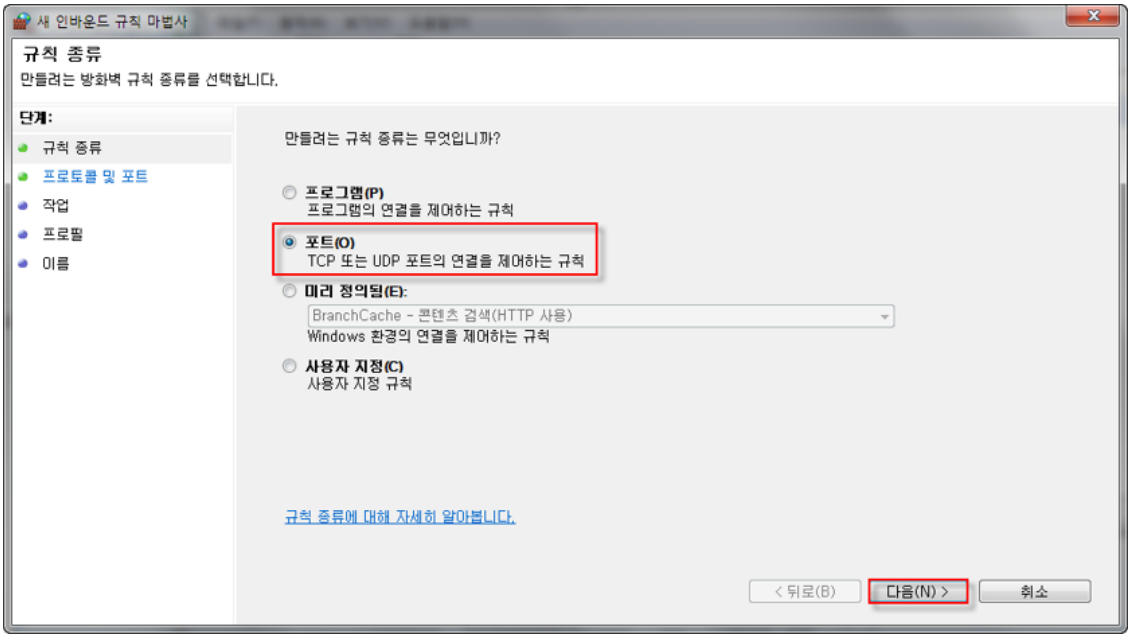
3. Windows 작업 표시줄의 **시작** > **설정** > **제어판** > **시스템 및 보안** > **Windows 방화벽**을 선택한 후 **고급 설정**을 선택합니다.



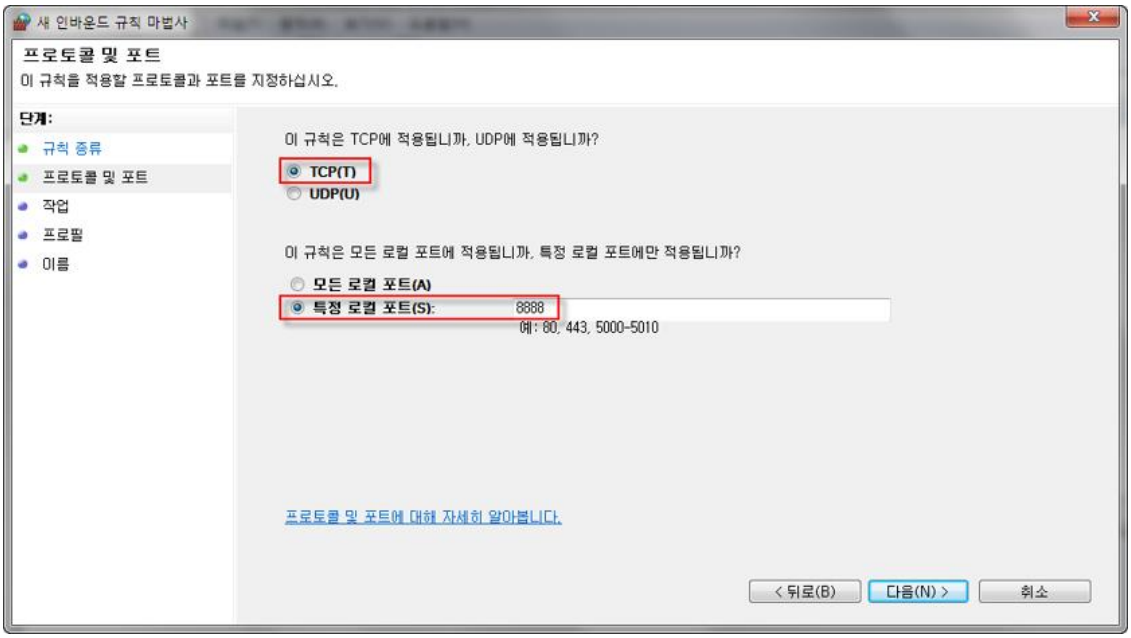
4. 좌측의 **인 바운드 규칙** 선택 후, 우측의 **새 규칙**을 선택합니다.



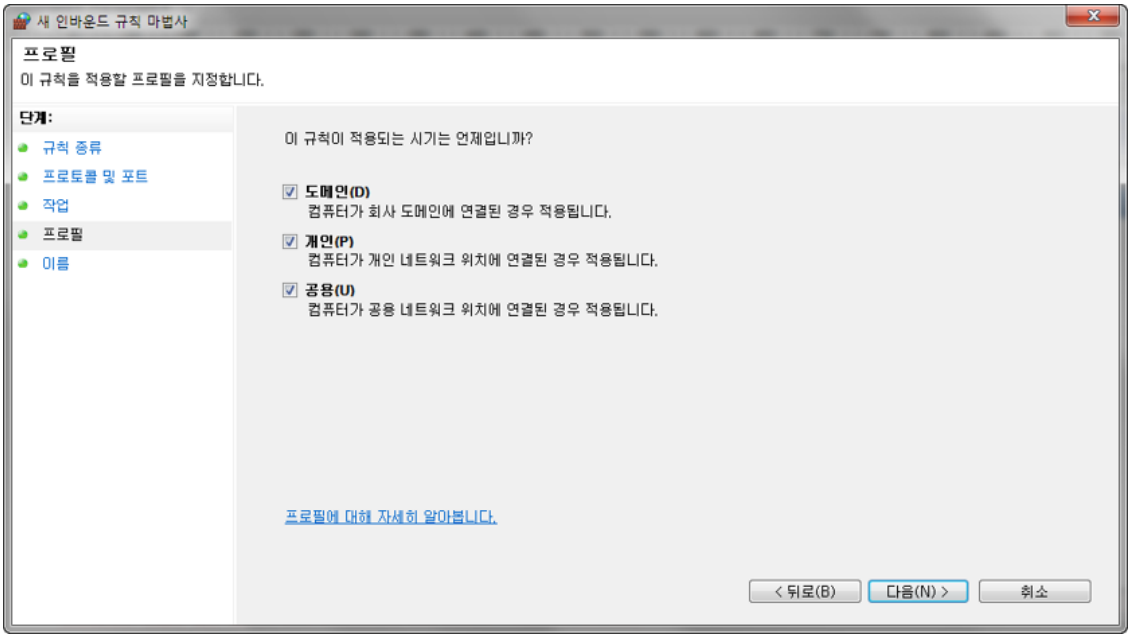
5. 규칙 종류에서 **포트(O)**를 선택 후 다음을 누릅니다.



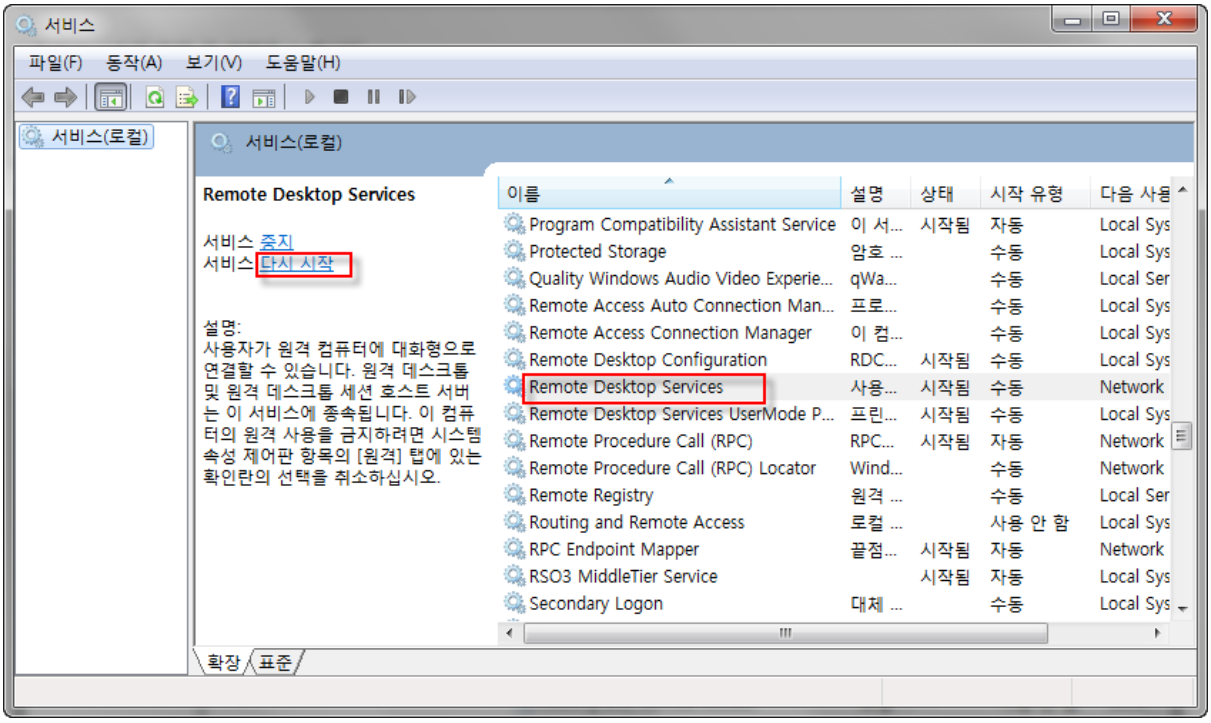
6. 프로토콜 및 포트에서 **TCP(T)**를 선택 후 **특정 로컬 포트(S)**에 설정한 포트 번호를 입력하고 다음을 누릅니다.



7. 작업에서 **연결 허용**을 선택합니다.
8. 프로필에서 다음과 같이 **도메인, 개인, 공용**에 모두 체크 표시한 후 **다음**을 클릭합니다.



9. 이름에서 내용을 입력 후 **마침**을 누릅니다.
10. Windows 작업 표시줄의 **시작** > **설정** > **제어판** > **시스템 및 보안** > **관리 도구**를 선택한 후 **서비스**를 더블 클릭하여 실행합니다.
11. **Remote Desktop Services**를 **다시 시작**합니다.



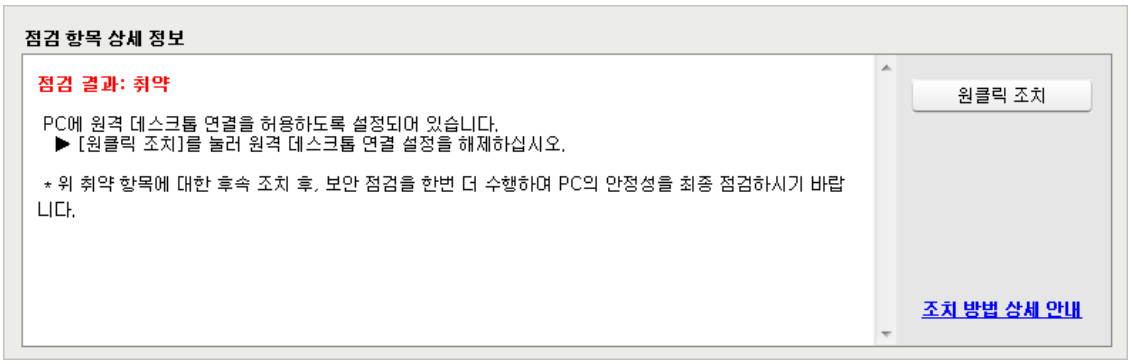
원격 데스크톱 사용 점검

원격 데스크톱 연결을 사용하고 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 원격 데스크톱 연결을 허용하지 않습니다.
- 취약: PC 에 원격 데스크톱 연결을 허용하도록 설정되어 있습니다. **원클릭 조치**를 눌러 원격 데스크톱 연결 설정을 해제하십시오.

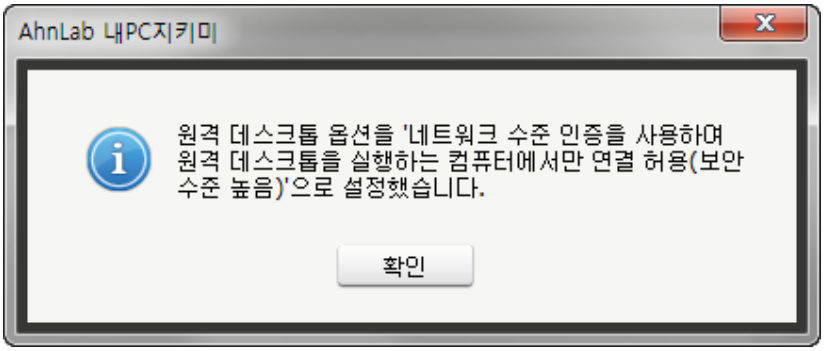


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 원격 데스크톱 연결을 허용하지 않도록 설정하면 다음과 같은 알림 창이 나타납니다.

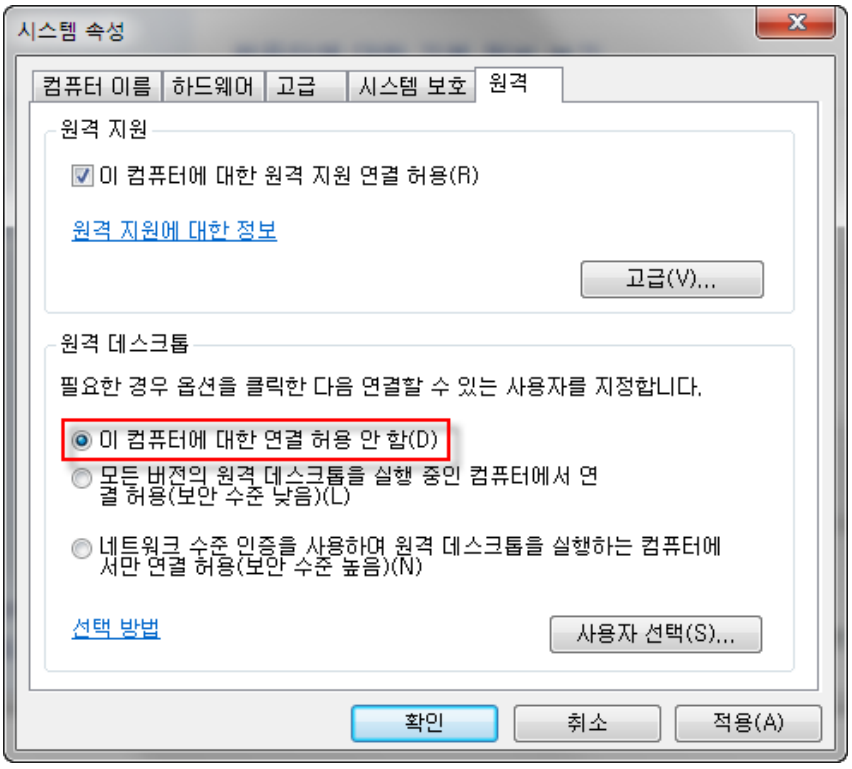


3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. Windows 작업 표시줄의 **시작** > **설정** > **제어판** > **시스템 및 보안** > **시스템**을 선택한 후 **고급 시스템 설정**을 선택합니다.

2. 상단의 탭에서 **원격** 탭을 선택 후 **이 컴퓨터에 대한 연결 허용 안 함(D)**으로 바꿉니다.



3. **적용**을 누른 다음 **확인** 버튼을 누릅니다.

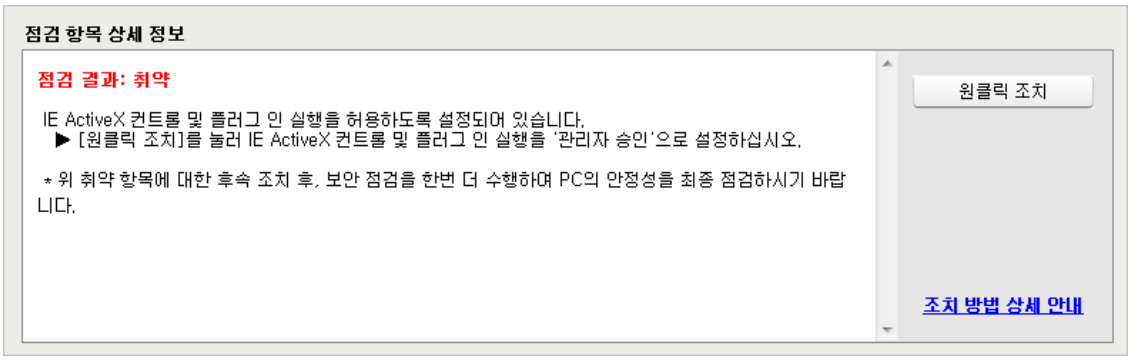
IE ActiveX 컨트롤 및 플러그 인 실행 점검

IE ActiveX 컨트롤 및 플러그 인 실행을 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: IE ActiveX 컨트롤 및 플러그 인 실행을 사용하지 않도록 설정되어 있습니다.
- 취약: IE ActiveX 컨트롤 및 플러그 인 실행을 허용하도록 설정되어 있습니다. **원클릭 조치**를 눌러 IE ActiveX 컨트롤 및 플러그 인 실행을 **관리자 승인**으로 설정하십시오.

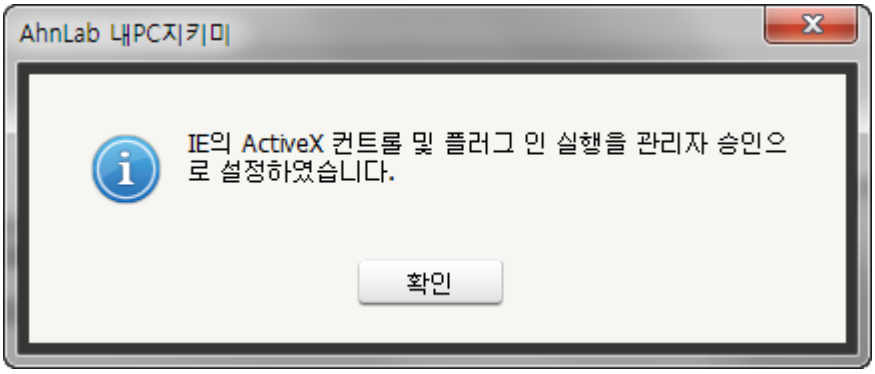


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

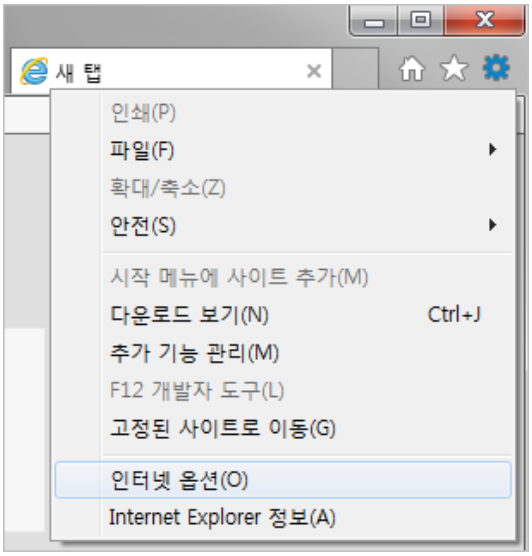
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 IE ActiveX 컨트롤 및 플러그 인 실행을 **관리자 승인**으로 설정하면 다음과 같은 알림 창이 나타납니다.



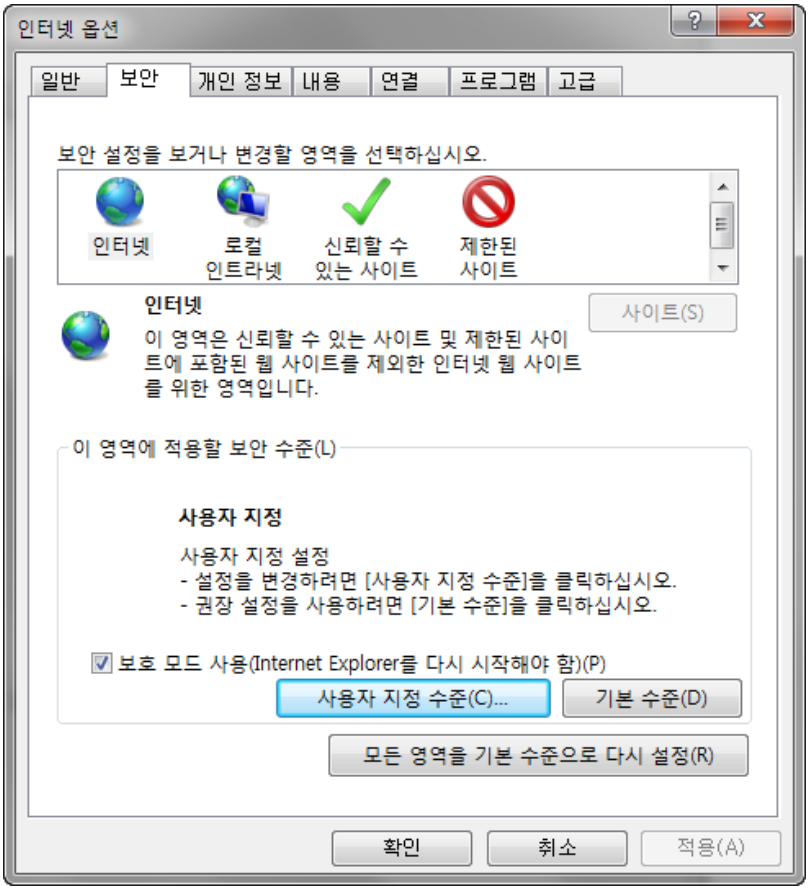
3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

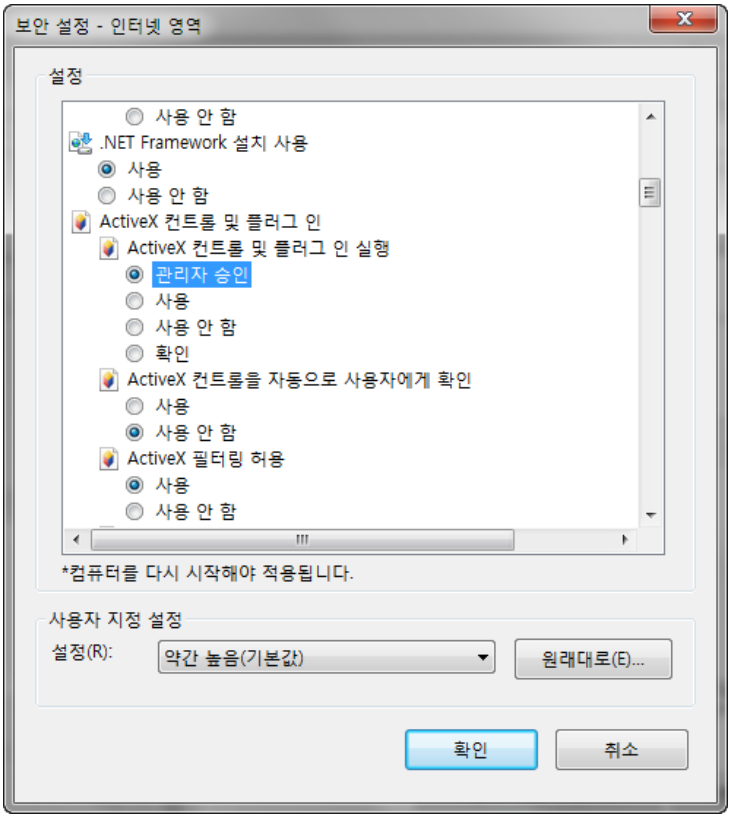
1. Internet Explorer를 실행하여 도구 메뉴를 눌러 **인터넷 옵션**을 선택합니다.



2. <인터넷 옵션>의 보안 탭에서 인터넷을 선택하고 **사용자 지정 수준**을 누릅니다.



3. ActiveX 컨트롤 및 플러그 인 실행에서 **사용** 설정 값을 제외한 설정 값을 선택합니다. **관리자 승인, 사용 안 함, 확인** 중에서 선택합니다.


보안 설정 - 인터넷 영역
설정
사용 안 함
.NET Framework 설치 사용
사용
사용 안 함
ActiveX 컨트롤 및 플러그 인
ActiveX 컨트롤 및 플러그 인 실행
관리자 승인
사용
사용 안 함
확인
ActiveX 컨트롤을 자동으로 사용자에게 확인
사용
사용 안 함
ActiveX 필터링 허용
사용
사용 안 함
*컴퓨터를 다시 시작해야 적용됩니다.
사용자 지정 설정
설정(R):
약간 높음(기본값)
원래대로(E)...
확인
취소

4. **확인**을 누릅니다.

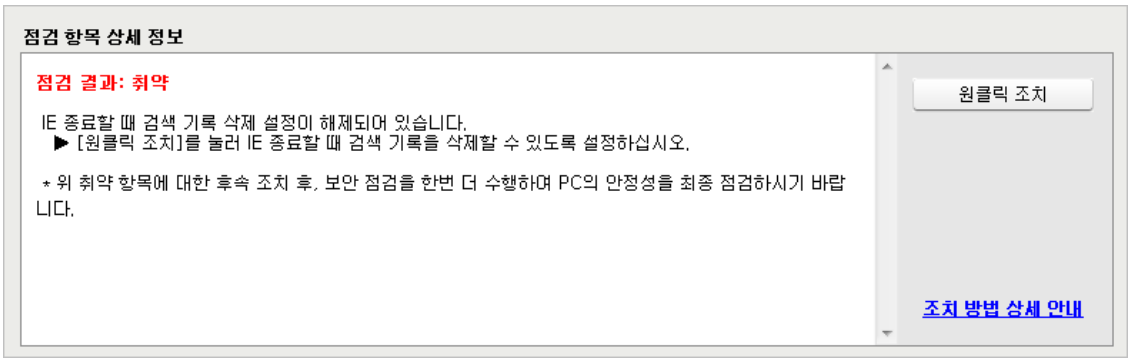
IE 종료할 때 검색 기록 삭제 점검

IE 종료할 때 검색 기록을 삭제하도록 설정되었는 지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: IE 종료할 때 검색 기록을 삭제하도록 설정되어 있습니다.
- 취약: IE 종료할 때 검색 기록 삭제 설정이 해제되어 있습니다. **원클릭 조치**를 눌러 IE 종료할 때 검색 기록을 삭제할 수 있도록 설정하십시오.

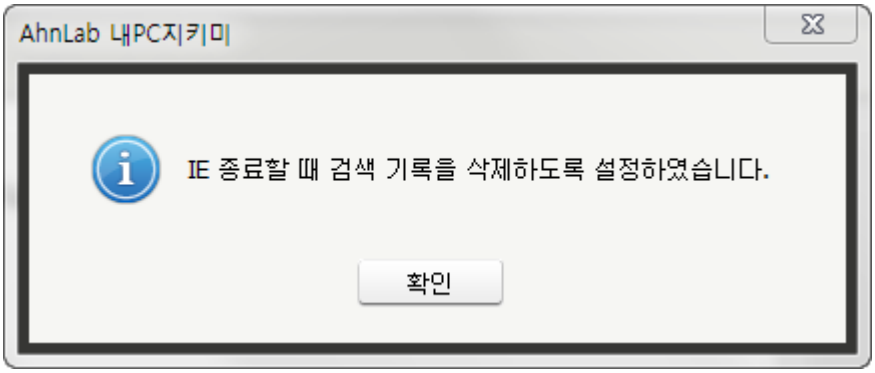


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

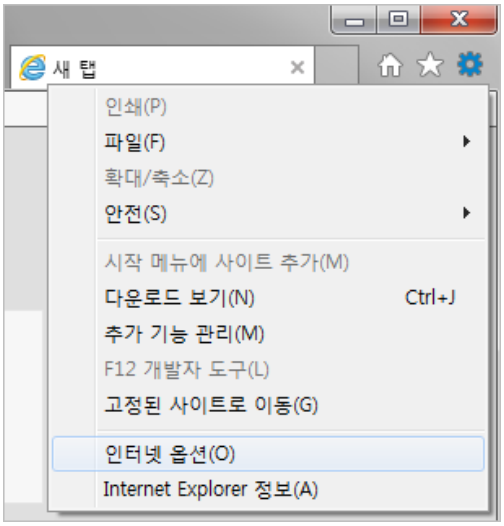
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 IE 종료할 때 검색 기록을 삭제하도록 설정하면 다음과 같은 알림 창이 나타납니다.



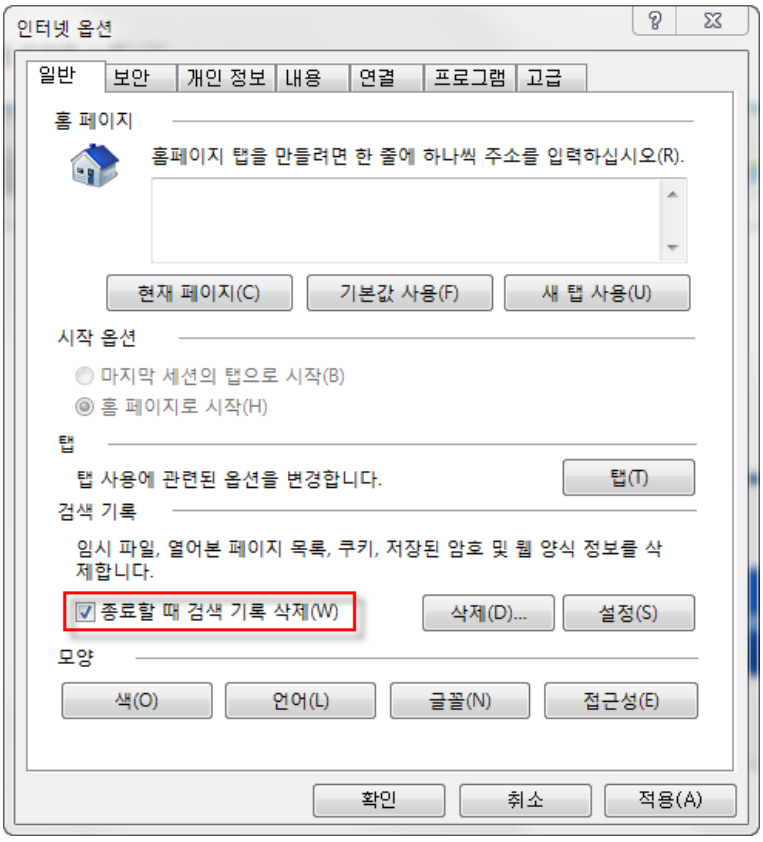
3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. Internet Explorer 를 실행하여 도구 메뉴를 눌러 **인터넷 옵션**을 선택합니다.



2. <인터넷 옵션>의 일반 탭에서 **종료할 때 검색 기록 삭제(W)**를 선택합니다.



3. **확인**을 누릅니다.

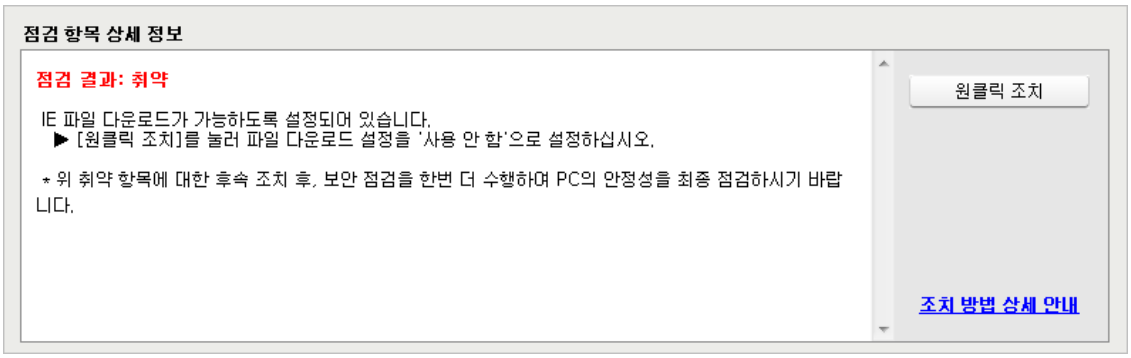
IE 파일 다운로드 사용 점검

IE 파일 다운로드 사용을 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: IE 파일 다운로드 기능을 사용하지 않도록 설정되어 있습니다.
- 취약: IE 파일 다운로드가 가능하도록 설정되어 있습니다. **원클릭 조치**를 눌러 파일 다운로드 설정을 '사용 안 함'으로 설정하십시오.

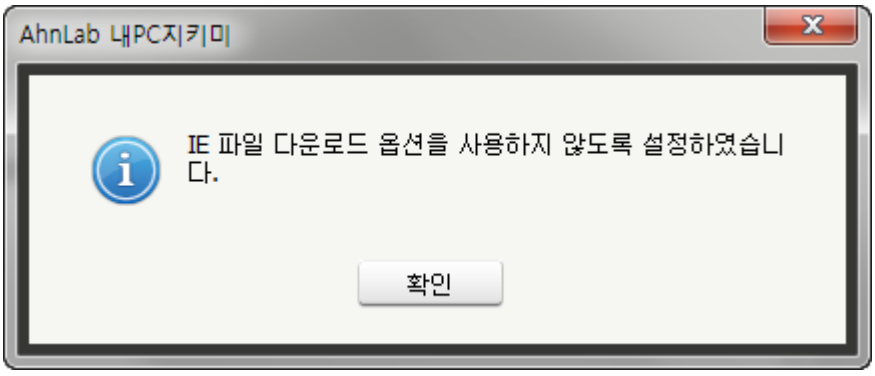


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

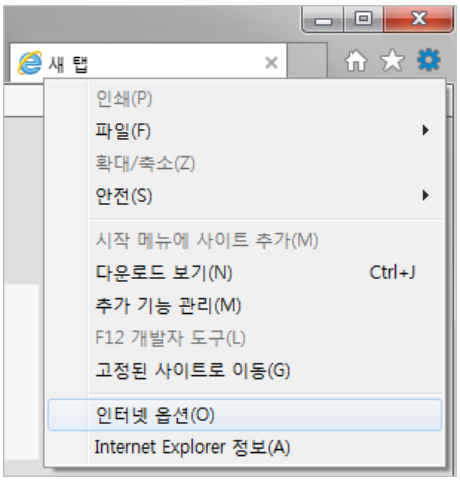
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 IE 파일 다운로드 기능을 **사용 안 함**으로 설정하면 다음과 같은 알림 창이 나타납니다.



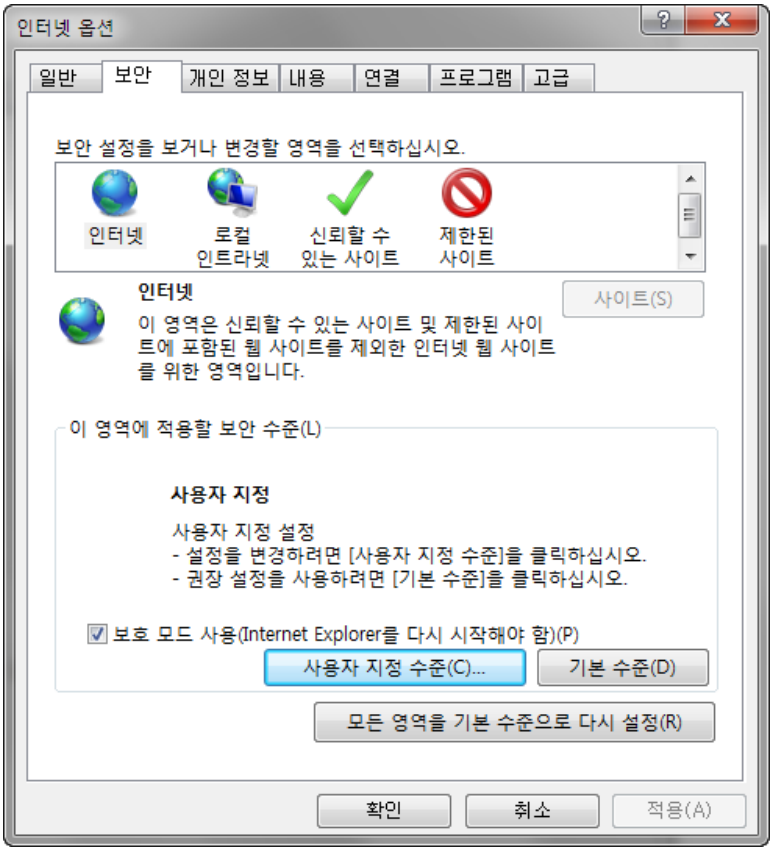
3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

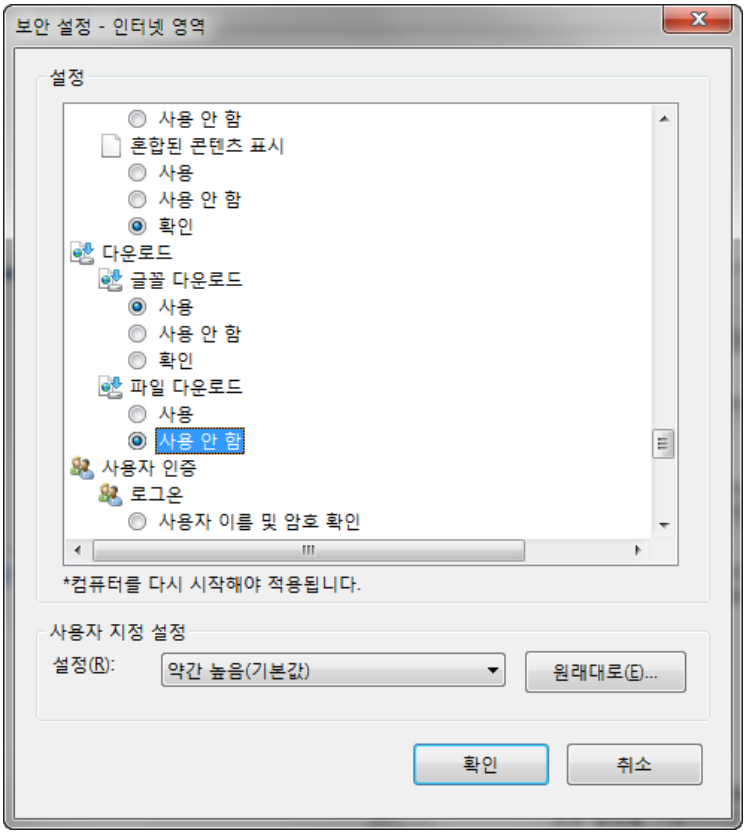
1. Internet Explorer를 실행하여 도구 메뉴를 눌러 **인터넷 옵션**을 선택합니다.



2. <인터넷 옵션>의 보안 탭에서 인터넷을 선택하고 **사용자 지정 수준**을 누릅니다.



3. <보안 설정>의 **다운로드** > **파일 다운로드** 설정을 **사용 안 함**으로 설정합니다.


보안 설정 - 인터넷 영역
설정
사용 안 함
혼합된 콘텐츠 표시
사용
사용 안 함
확인
다운로드
글꼴 다운로드
사용
사용 안 함
확인
파일 다운로드
사용
사용 안 함
사용자 인증
로그온
사용자 이름 및 암호 확인
*컴퓨터를 다시 시작해야 적용됩니다.
사용자 지정 설정
설정(R):
약간 높음(기본값)
원래대로(E)...
확인
취소

4. **확인**을 누릅니다.

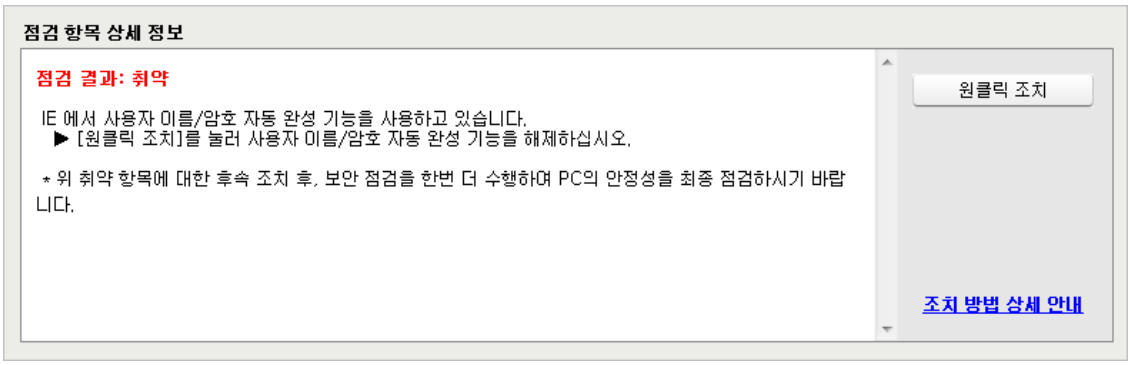
IE 사용자 이름/암호 자동 완성 설정 점검

IE 에서 사용자의 ID 와 패스워드 양식을 저장하여 자동 완성되도록 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: IE 에서 사용자 이름/암호 자동 완성을 사용하지 않습니다.
- 취약: IE 에서 사용자 이름/암호 자동 완성 기능을 사용하고 있습니다. **원클릭 조치**를 눌러 사용자 이름/암호 자동 완성 기능을 해제하십시오.

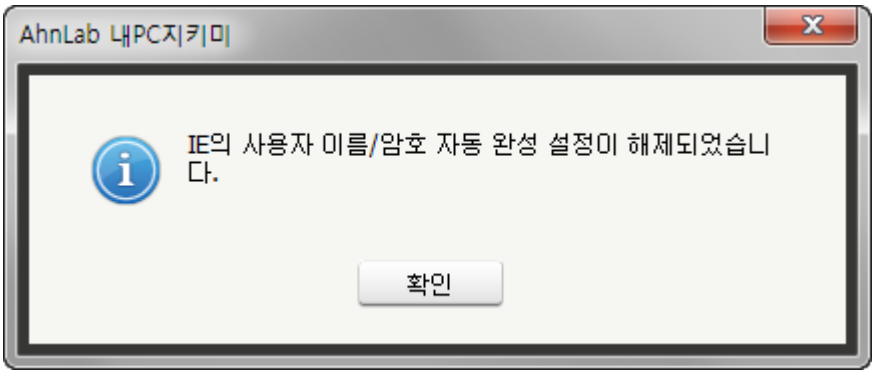


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

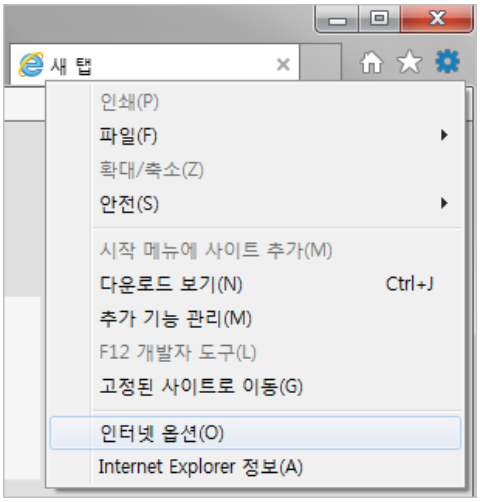
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 IE 에서 사용자 이름/암호 자동 완성 기능을 사용하지 않도록 설정하면 다음과 같은 알림 창이 나타납니다.



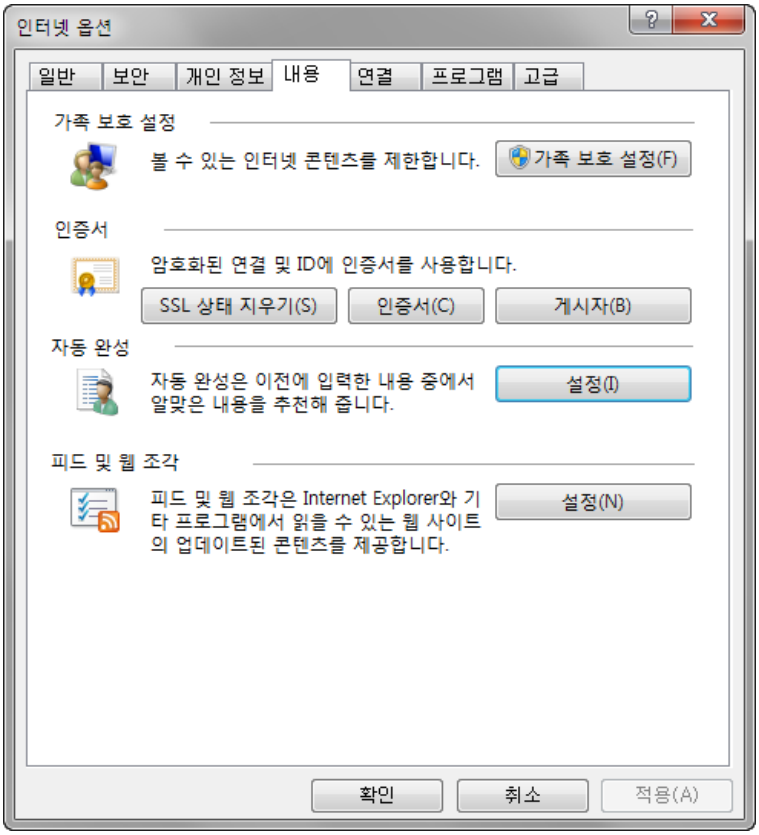
3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

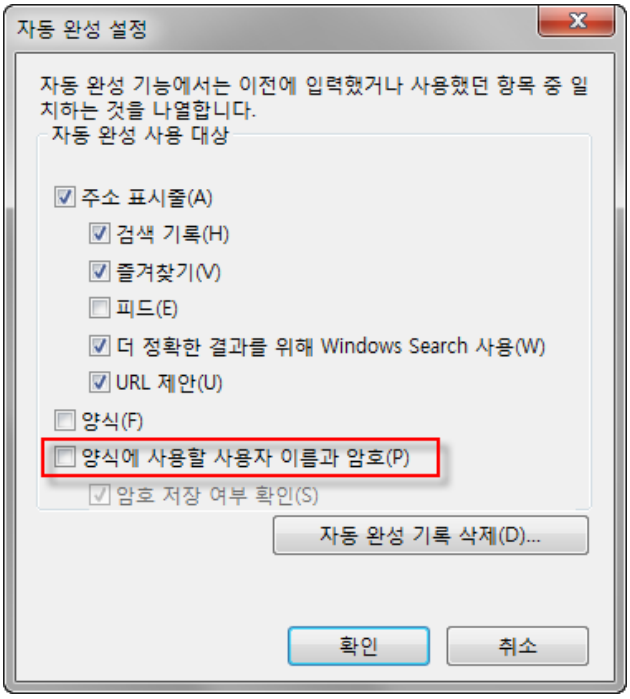
1. Internet Explorer 를 실행하여 도구 메뉴를 눌러 **인터넷 옵션**을 선택합니다.



2. <인터넷 옵션>의 **내용 탭을** 선택한 후, 자동 완성 기능의 **설정**을 누릅니다.



3. <자동 완성 설정>에서 **양식에 사용할 사용자 이름과 암호(P)**를 선택 해제합니다.


자동 완성 설정
자동 완성 기능에서는 이전에 입력했거나 사용했던 항목 중 일치하는 것을 나열합니다.
자동 완성 사용 대상
주소 표시줄(A)
검색 기록(H)
즐겨찾기(V)
피드(E)
더 정확한 결과를 위해 Windows Search 사용(W)
URL 제안(U)
양식(F)
양식에 사용할 사용자 이름과 암호(P)
암호 저장 여부 확인(S)
자동 완성 기록 삭제(D)...
확인
취소

4. **확인**을 누릅니다.

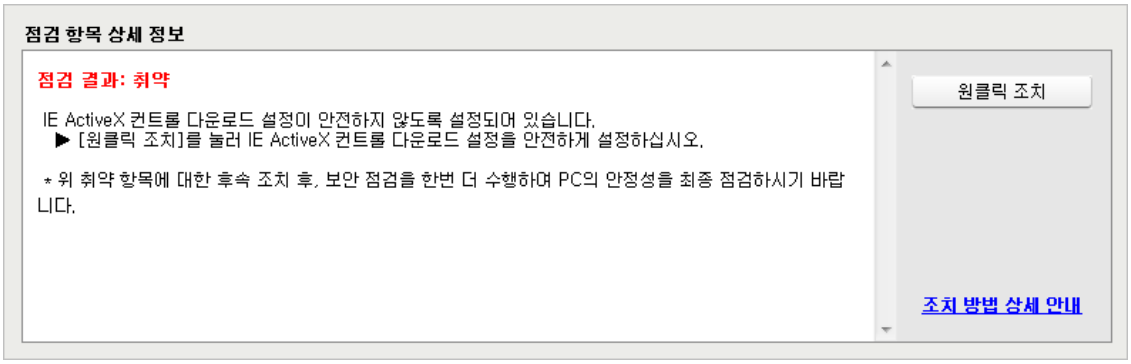
IE ActiveX 컨트롤 다운로드 설정 점검

IE 에서 ActiveX 컨트롤 다운로드 설정을 점검합니다. 서명 된/서명 안 된 ActiveX 컨트롤 다운로드 설정이 하나라도 **사용**으로 되어 있으면 취약으로 진단됩니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 IE ActiveX 컨트롤 다운로드 설정이 안전하게 설정되어 있습니다.
- 취약: IE ActiveX 컨트롤 다운로드 설정이 안전하지 않도록 설정되어 있습니다. 원클릭 조치를 눌러 IE 의 서명된/서명 안 된 ActiveX 컨트롤 다운로드 설정을 '확인'으로 설정하십시오.

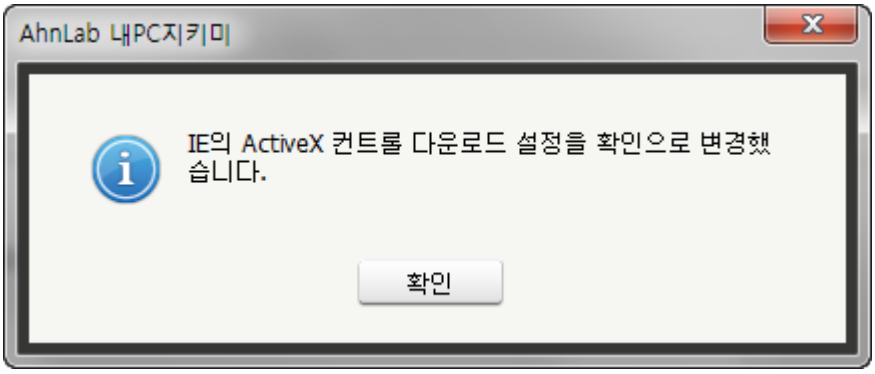


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

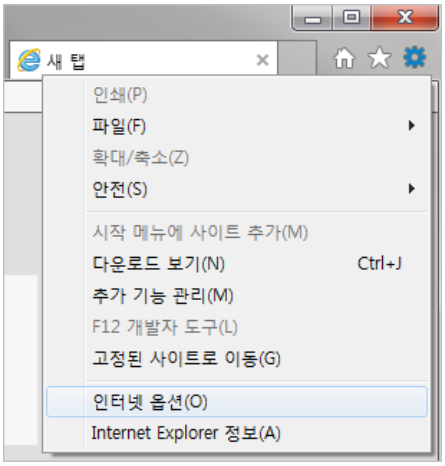
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 IE 의 ActiveX 컨트롤 다운로드 설정을 다음과 설정하면 알림 창이 나타납니다.
   - 서명 안 된 ActiveX 컨트롤 다운로드 설정을 **확인**으로 변경합니다.
   - 서명된 ActiveX 컨트롤 다운로드 설정을 **확인**으로 변경합니다.



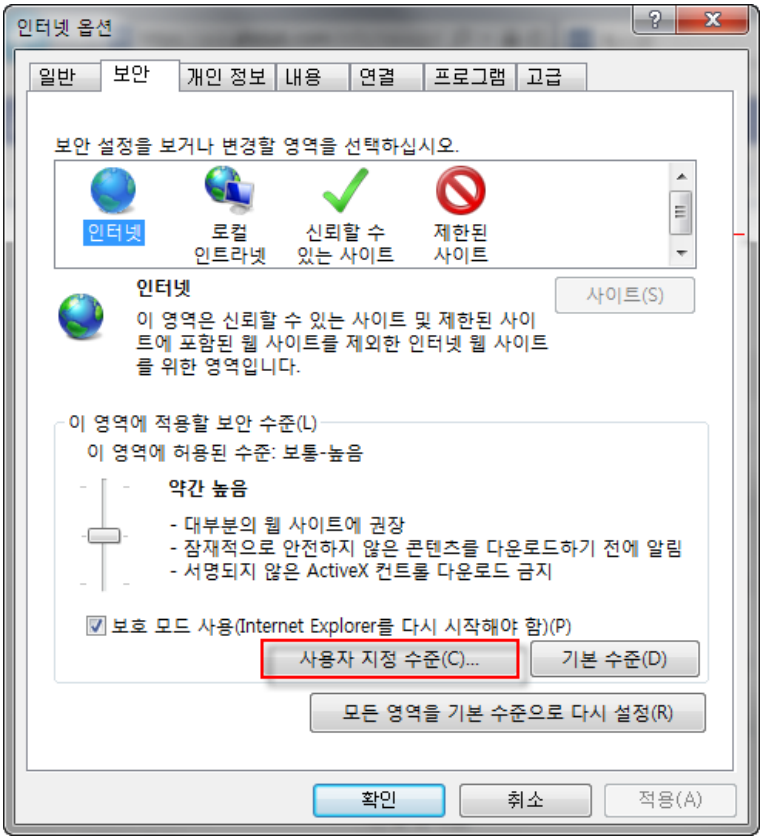
3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

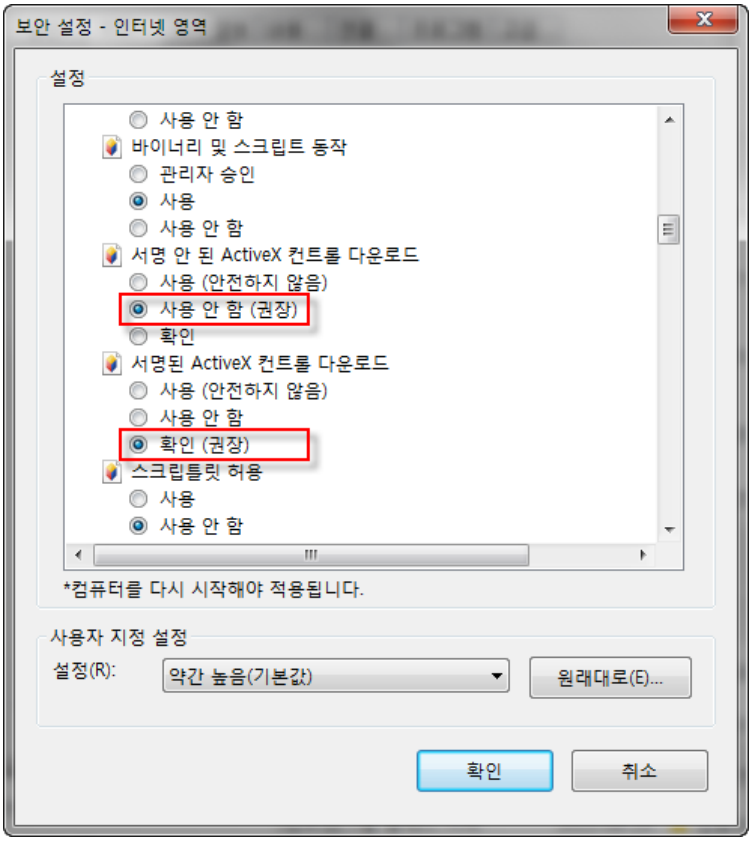
1. Internet Explorer를 실행하여 도구 메뉴를 눌러 **인터넷 옵션**을 선택합니다.



2. **보안** 탭의 **사용자 지정 수준**을 클릭합니다.



3. ActiveX 컨트롤 및 플러그 인 영역의 **서명 안 된 ActiveX 컨트롤 다운로드/서명된 ActiveX 컨트롤 다운로드**를 **권장**으로 설정합니다.


보안 설정 - 인터넷 영역
설정
사용 안 함
바이너리 및 스크립트 동작
관리자 승인
사용
사용 안 함
서명 안 된 ActiveX 컨트롤 다운로드
사용 (안전하지 않음)
사용 안 함 (권장)
확인
서명된 ActiveX 컨트롤 다운로드
사용 (안전하지 않음)
사용 안 함
확인 (권장)
스크립팅 허용
사용
사용 안 함
*컴퓨터를 다시 시작해야 적용됩니다.
사용자 지정 설정
설정(R):
약간 높음(기본값)
원래대로(E)...
확인
취소

4. **확인**을 누릅니다.

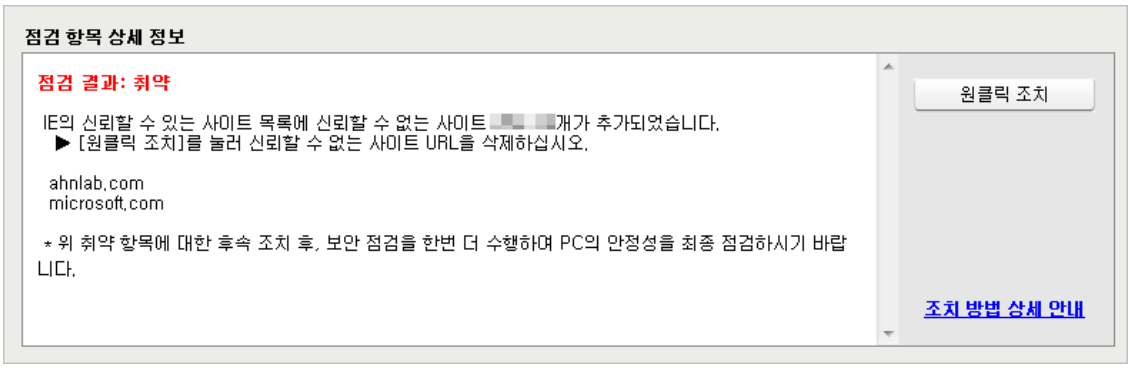
IE 신뢰할 수 있는 사이트 목록의 취약성 점검

IE 에 설정되어 있는 신뢰할 수 있는 사이트 목록에 취약성이 존재하는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: IE 의 **신뢰할 수 있는 사이트 목록**에 취약점이 존재하지 않습니다.
- 취약: IE 의 **신뢰할 수 있는 사이트 목록**에 신뢰할 수 없는 사이트의 URL 이 추가되어 있습니다. **원클릭 조치**를 눌러 신뢰할 수 없는 사이트 URL 을 삭제하십시오.

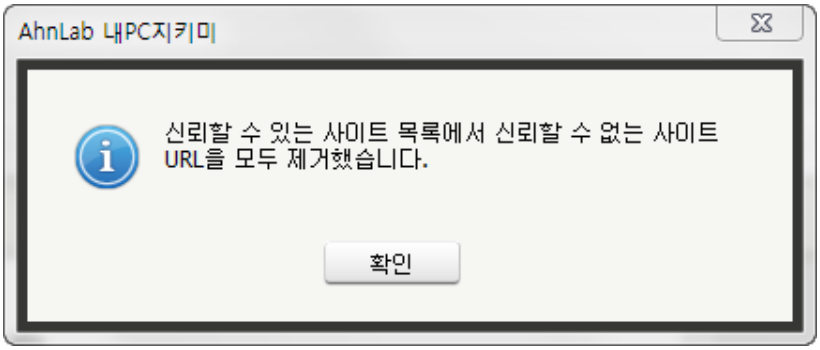


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

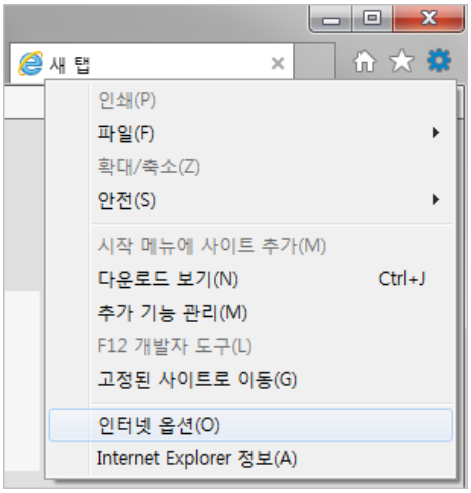
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 설정을 변경하면 다음과 같은 알림 창이 나타납니다.



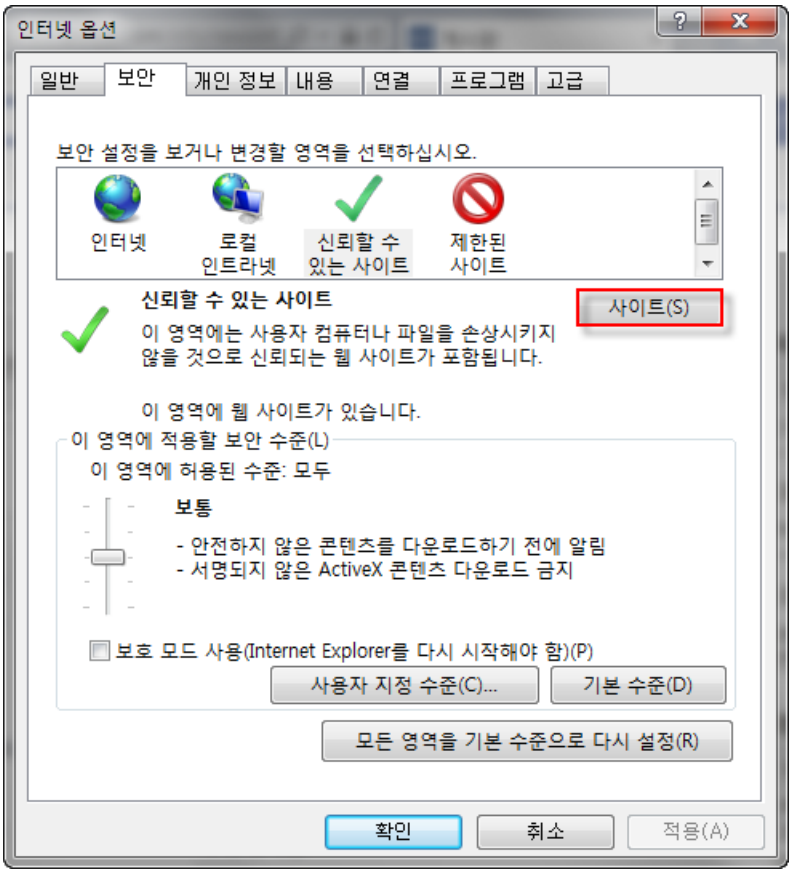
3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

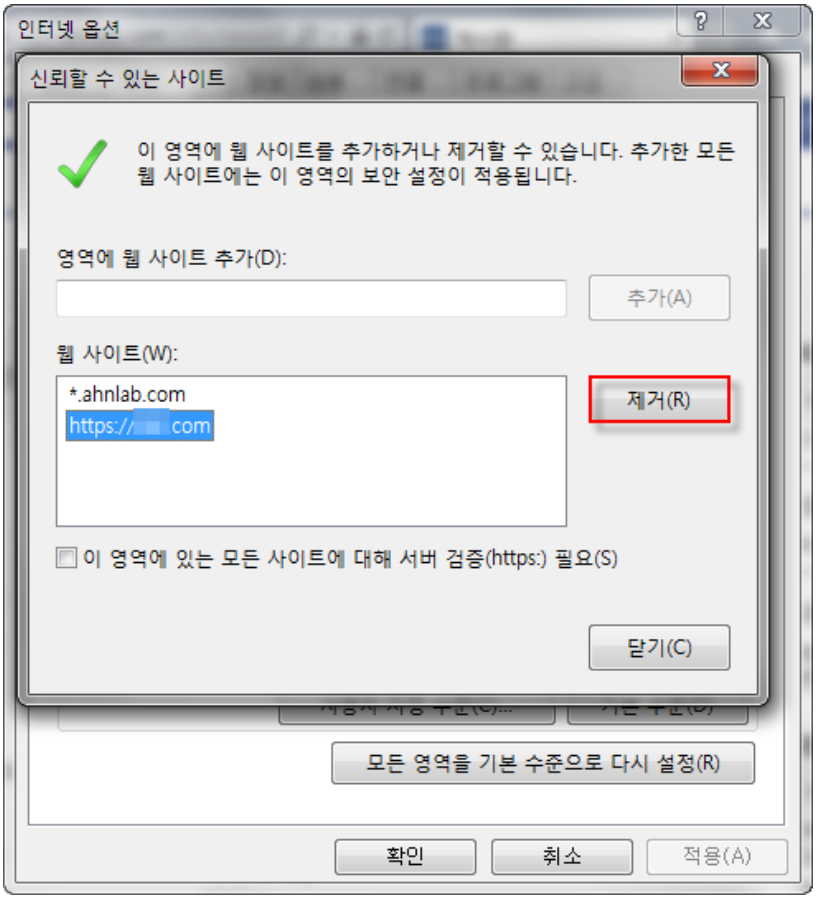
1. Internet Explorer를 실행하여 도구 메뉴를 눌러 **인터넷 옵션**을 선택합니다.



2. **보안** 탭의 **신뢰할 수 있는 사이트** 클릭 후 **사이트(S)**를 클릭합니다.



3. **신뢰할 수 없는 사이트**를 클릭 후 **제거**를 누릅니다.


인터넷 옵션
신뢰할 수 있는 사이트
이 영역에 웹 사이트를 추가하거나 제거할 수 있습니다. 추가한 모든 웹 사이트에는 이 영역의 보안 설정이 적용됩니다.
영역에 웹 사이트 추가(D):
추가(A)
웹 사이트(W):
*.ahnlab.com
https:// com
제거(R)
이 영역에 있는 모든 사이트에 대해 서버 검증(https:) 필요(S)
닫기(C)
모든 영역을 기본 수준으로 다시 설정(R)
확인
취소
적용(A)

4. **확인**을 누릅니다.

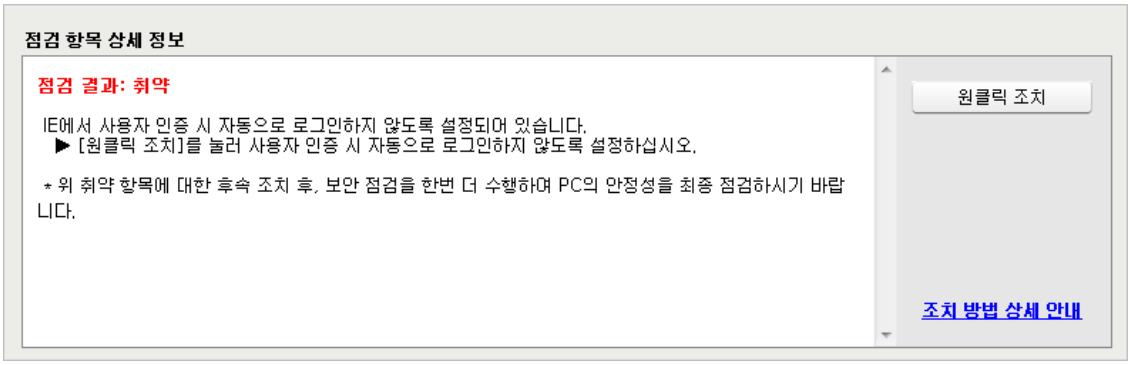
IE 사용자 인증 시 자동 로그온 설정 점검

IE 에서 사용자 인증을 요구할 때, 사용자 계정과 암호가 저장되어 자동으로 로그온할 수 있도록 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: IE 에서 사용자 인증 시 자동으로 로그인하지 않도록 설정되어 있습니다.
- 취약: IE 에서 사용자 인증 시 자동으로 로그인 하도록 설정되어 있습니다. **원클릭 조치**를 눌러 사용자 인증 시 자동으로 로그인하지 않도록 설정하십시오.

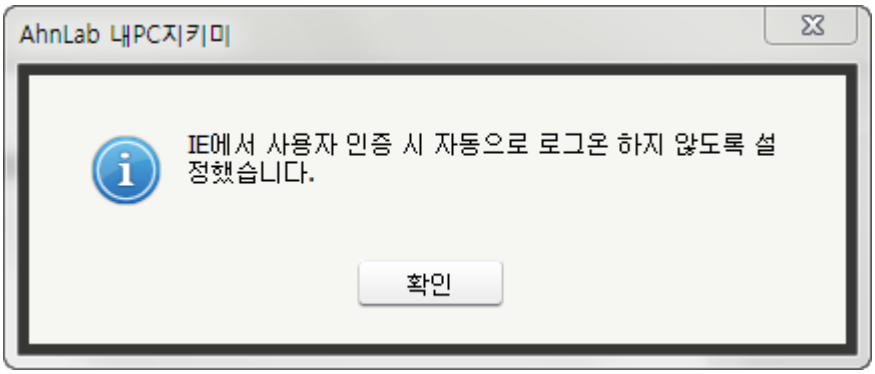


조치 방법

조치 방법에는 **원클릭 조치** 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 **사용자 조치** 방법이 있습니다.

[원클릭 조치]

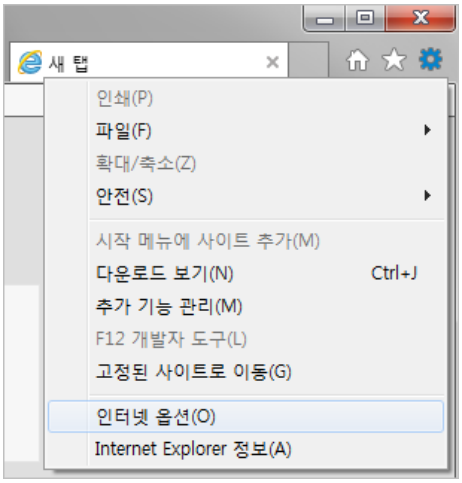
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 사용자 인증 로그온 시, 사용자 이름과 암호를 확인하도록 설정하면 다음과 같은 알림 창이 나타납니다.



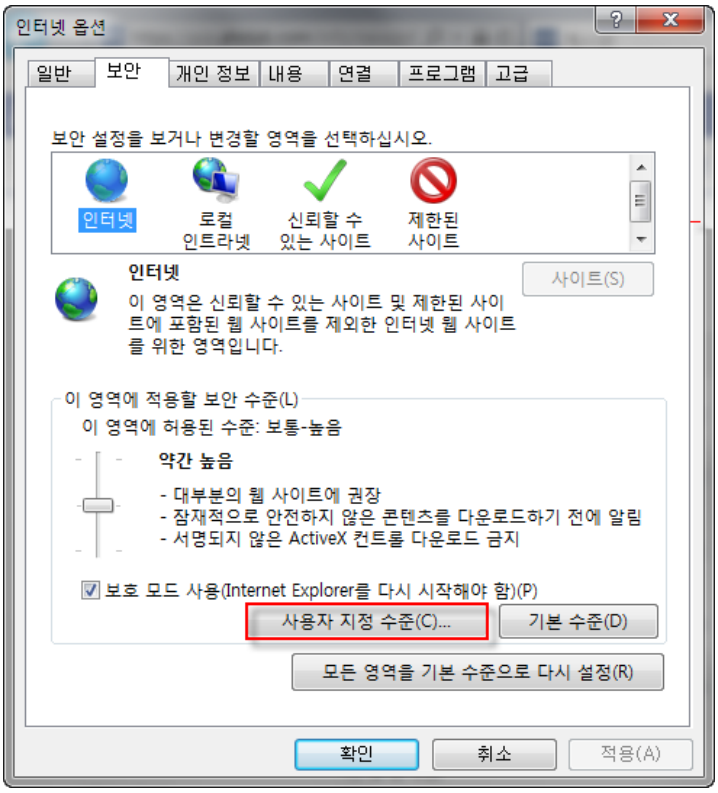
3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

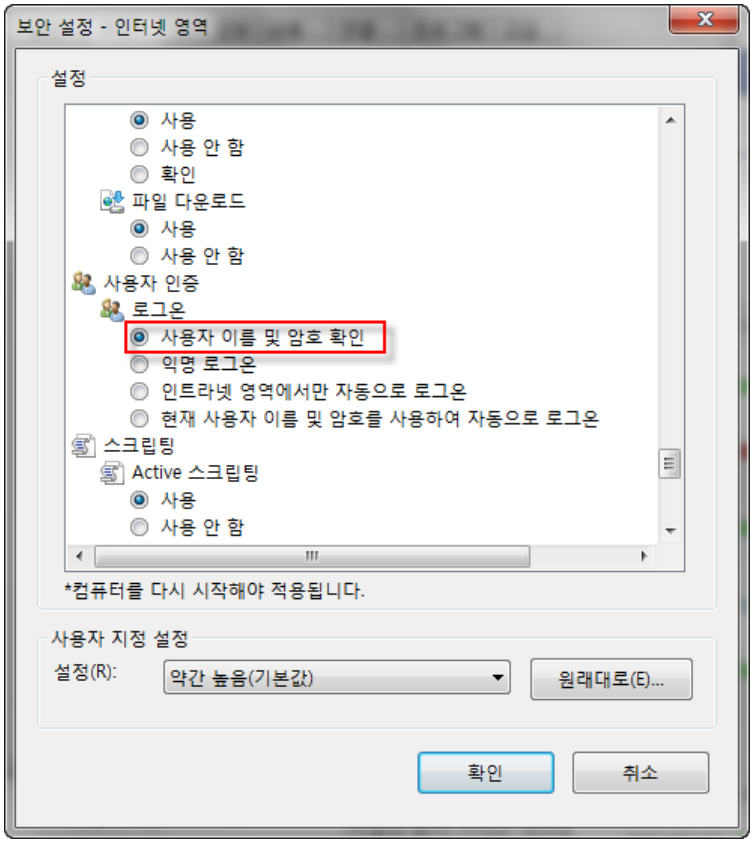
1. Internet Explorer를 실행하여 도구 메뉴를 눌러 **인터넷 옵션**을 선택합니다.



2. **보안** 탭의 **사용자 지정 수준(C)...**을 클릭합니다.



3. **사용자 인증 영역**의 **사용자 이름 및 암호 확인**을 클릭 후 **확인**을 누릅니다.


보안 설정 - 인터넷 영역
설정
사용
사용 안 함
확인
파일 다운로드
사용
사용 안 함
사용자 인증
로그온
사용자 이름 및 암호 확인
익명 로그온
인트라넷 영역에서만 자동으로 로그온
현재 사용자 이름 및 암호를 사용하여 자동으로 로그온
스크립팅
Active 스크립팅
사용
사용 안 함
*컴퓨터를 다시 시작해야 적용됩니다.
사용자 지정 설정
설정(R):
약간 높음(기본값)
원래대로(E)...
확인
취소

4. **확인**을 누릅니다.

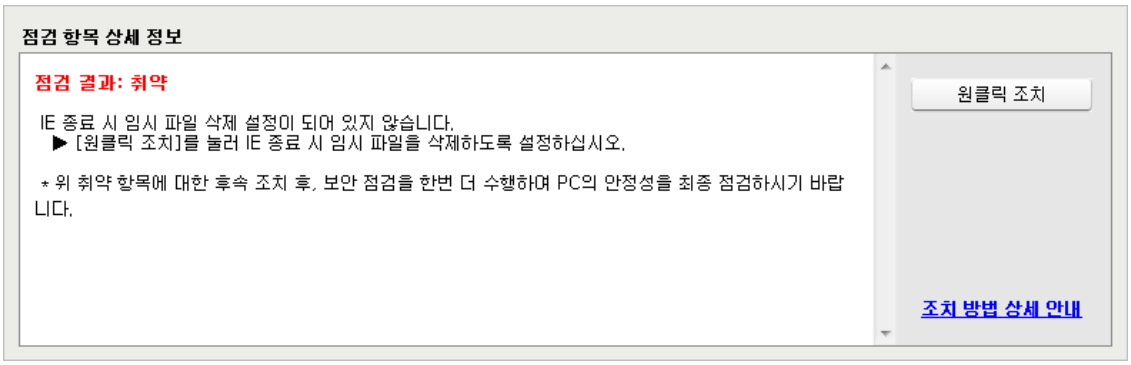
IE 종료 시 임시 인터넷 파일 삭제 점검

IE 종료 시 자동으로 임시 파일을 삭제하도록 설정되어 있는지 여부를 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: IE 종료 시 임시 인터넷 파일을 삭제하도록 설정되어 있습니다.
- 취약: IE 종료 시 임시 인터넷 파일 삭제 설정이 되어 있지 않습니다. **원클릭 조치**를 눌러 IE 종료 시 임시 파일을 삭제하도록 설정하십시오.

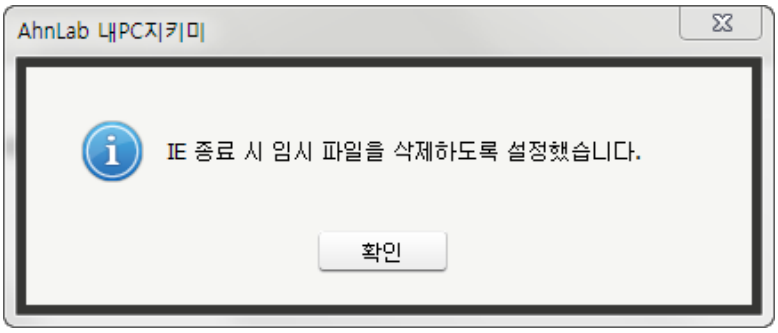


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

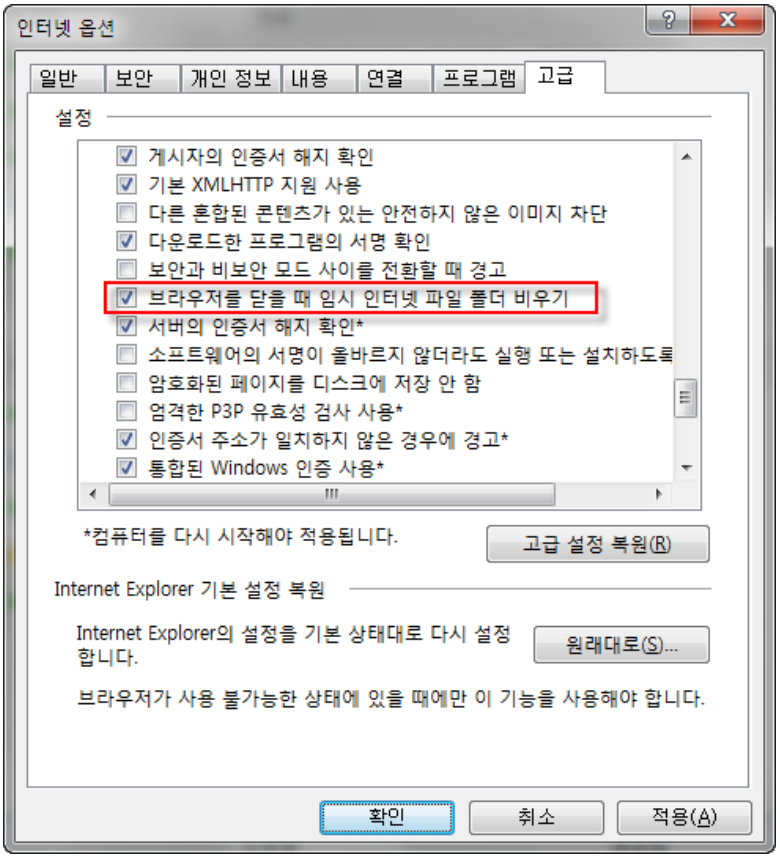
1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 IE 종료 시 임시 인터넷 파일을 삭제하도록 설정하면 다음과 같은 알림 창이 나타납니다.



3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. Internet Explorer를 실행하여 도구 메뉴를 눌러 **인터넷 옵션**을 선택합니다.
2. 인터넷 옵션 창에서 **고급** 탭을 선택하고, 스크롤을 내리면 **보안** 항목란이 있습니다. **브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기**에 체크하고 **적용**을 누릅니다.


인터넷 옵션
일반
보안
개인 정보
내용
연결
프로그램
고급
설정
게시자의 인증서 해지 확인
기본 XMLHTTP 지원 사용
다른 혼합된 콘텐츠가 있는 안전하지 않은 이미지 차단
다운로드한 프로그램의 서명 확인
보안과 비보안 모드 사이를 전환할 때 경고
브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기
서버의 인증서 해지 확인*
소프트웨어의 서명이 올바르지 않더라도 실행 또는 설치하도록
암호화된 페이지를 디스크에 저장 안 함
엄격한 P3P 유효성 검사 사용*
인증서 주소가 일치하지 않은 경우에 경고*
통합된 Windows 인증 사용*
*컴퓨터를 다시 시작해야 적용됩니다.
고급 설정 복원(R)
Internet Explorer 기본 설정 복원
Internet Explorer의 설정을 기본 상태대로 다시 설정합니다.
원래대로(S)...
브라우저가 사용 불가능한 상태에 있을 때에만 이 기능을 사용해야 합니다.
확인
취소
적용(A)

3. **확인**을 누릅니다.

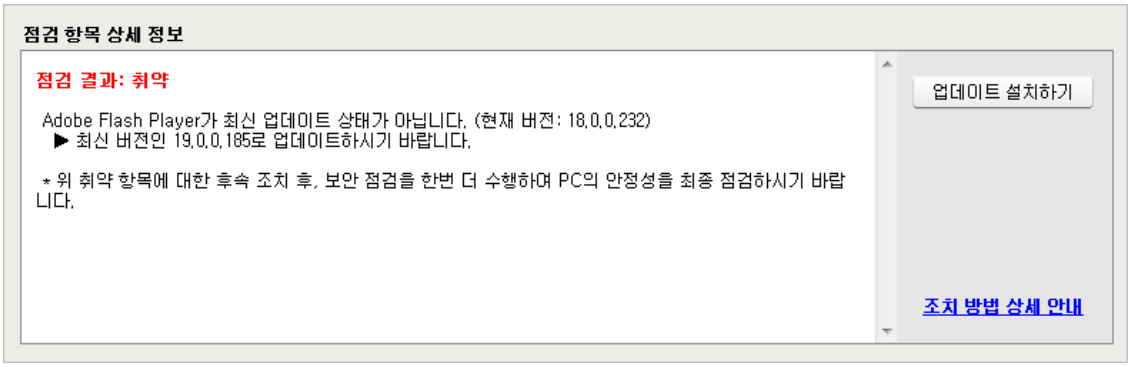
Adobe Flash Player 최신 업데이트 점검

Adobe Flash Player 가 최신으로 업데이트되어 있는 지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: Adobe Flash Player 가 최신으로 업데이트되어 있습니다.
- 취약: Adobe Flash Player 가 최신 업데이트 상태가 아닙니다. **업데이트 설치하기**를 눌러 최신 버전의 보안 업데이트를 설치하십시오.



조치 방법

점검 결과가 **취약**일 때, APM 라이선스가 없는 경우와 APM 라이선스가 있는 경우에 따라 다음과 같이 조치하여 주시기 바랍니다.

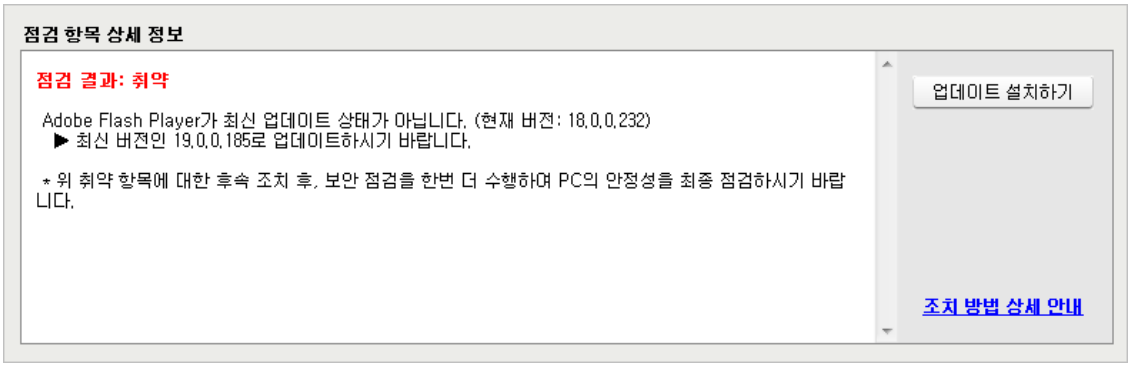
[APM 라이선스가 없는 경우]

1. 점검 항목 상세 정보에서 **업데이트 설치하기**를 누릅니다.
2. Adobe 홈페이지에서 최신 파일을 다운로드 하여 설치합니다.

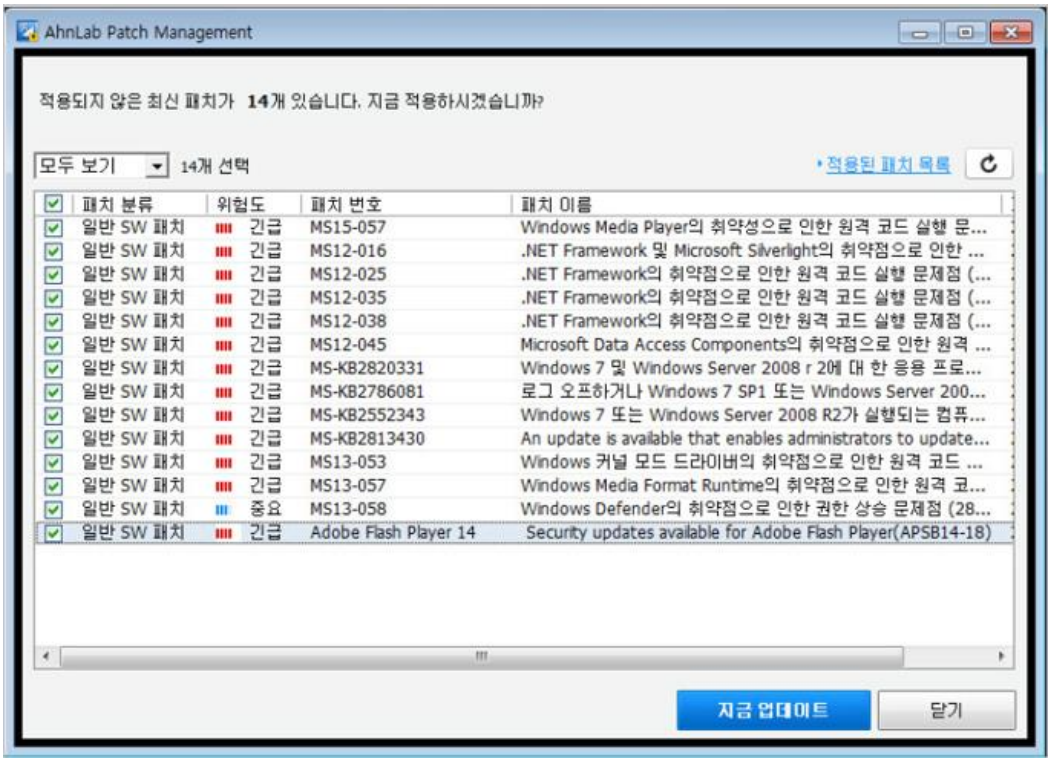
[APM 라이선스가 있는 경우]

APM 제품을 통해 적용되지 않은 패치 목록을 확인하고 최신 보안 패치를 적용할 수 있습니다.

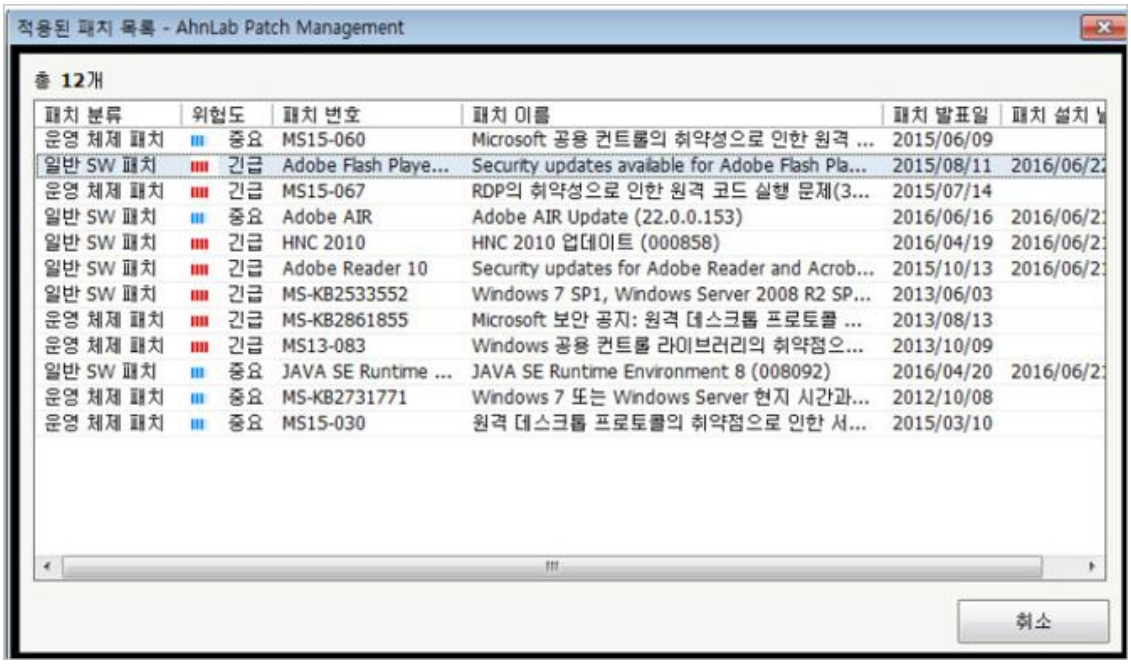
1. 업데이트 설치하기를 누릅니다.



2. APM이 실행되며 <패치 정보 보기>에서 현재 사용자 PC에 적용되지 않은 패치 목록을 확인할 수 있습니다.



3. **지금 업데이트**를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.
4. 패치 적용이 완료되면 화면 상단의 **적용된 패치 목록**을 눌러 설치된 패치 정보를 확인할 수 있습니다.



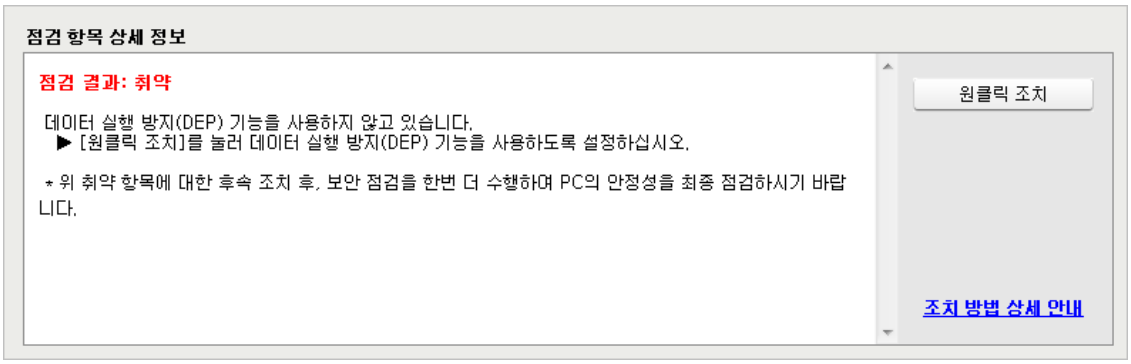
데이터 실행 방지(DEP) 사용 점검

Zeroday 공격 위험을 최소화하기 위하여 데이터 실행 방지(DEP) 기능을 사용하고 있는지를 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: 데이터 실행 방지(DEP) 기능을 사용하도록 설정되어 있습니다.
- 취약: 데이터 실행 방지(DEP) 기능을 사용하지 않고 있습니다. **원클릭 조치**를 눌러 데이터 실행 방지(DEP) 기능을 사용하도록 설정하십시오.

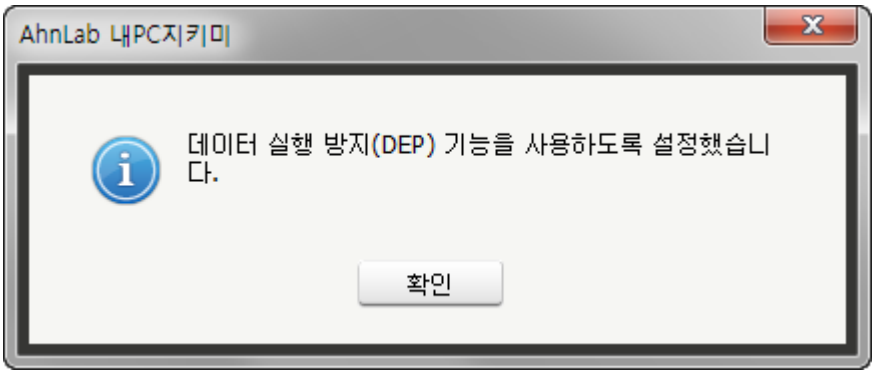


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 데이터 실행 방지(DEP)기능을 사용하도록 설정하면 다음과 같은 알림 창이 나타납니다.



3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. 시작 > 모든 프로그램 > 보조 프로그램에서 명령 프롬프트를 마우스 오른쪽 버튼으로 클릭하여, 관리자 권한으로 실행합니다.
2. <명령 프롬프트>가 실행되면 다음과 같이 명령어를 입력합니다.

```
C:\Windows\system32>bcdedit
```

- nx 값이 **OptIn, OptOut, AlwaysOn** 인 경우 안전으로 진단합니다.

- nx 값이 **AlwaysOff** 인 경우는 취약으로 진단합니다.

3. nx값이 **AlwaysOff**으로 설정되어 있는 경우 <명령 프롬프트>에서 다음과 명령어를 입력합니다.

```
C:\Windows\system32>bcdedit /set nx OptIn
```

개인 정보 미처리 파일 개수 초과 점검

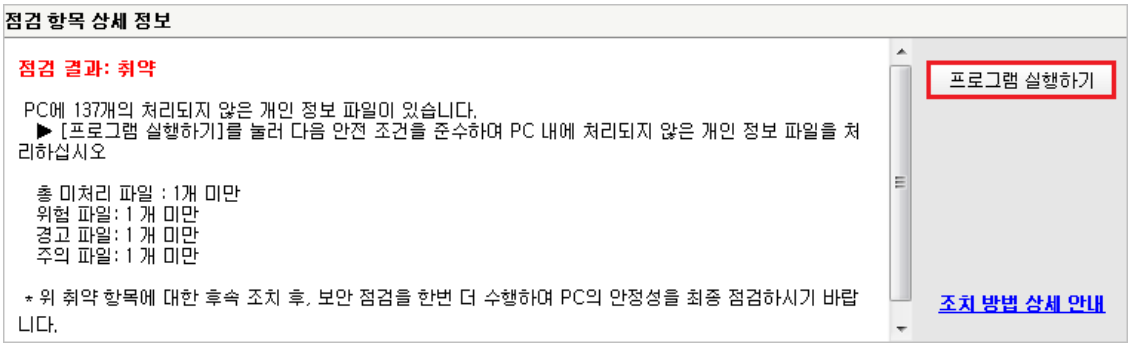
사용자 PC 에 처리되지 않은 개인 정보 보유 파일이 안전 조건을 초과하여 존재하는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

[AhnLab Privacy Management 라이선스가 있는 경우]

- 안전: PC 에 처리되지 않은 개인 정보 파일 개수가 안전 조건을 초과하지 않았습니다.
- 취약: PC 에 처리되지 않은 개인 정보 파일이 있습니다. **프로그램 실행하기**를 눌러 다음 안전 조건을 준수하여 PC 내에 처리되지 않은 개인 정보 파일을 처리하십시오.



조치 방법

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

1. 점검 항목 상세 정보에서 **프로그램 실행하기**를 누릅니다.
2. **프로그램 실행하기**를 누르면 다음과 같이 AhnLab Privacy Management Agent 가 실행됩니다.

3. **개인정보 처리 현황**에서 격리, 암호화, 예외 처리가 되지 않은 **미처리 개인 정보 파일**을 확인합니다.
4. 미처리 파일의 특성에 따라 격리, 암호화, 예외 처리를 합니다.

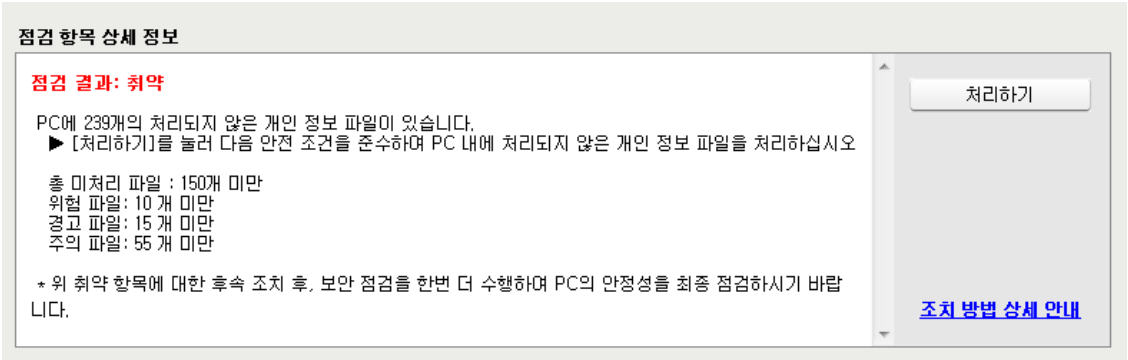
참고

AhnLab Privacy Management 라이선스가 없는 경우에는 점검을 수행할 수 없습니다. 해당 항목을 점검하려면 관련 제품의 라이선스를 구입해야 합니다.

[AhnLab Privacy Management 라이선스가 없는 경우]

AhnLab Privacy Management 라이선스가 없지만, 관리 콘솔에서 내 PC 지키미의 **개인 정보 검색** 기능을 사용하도록 설정된 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

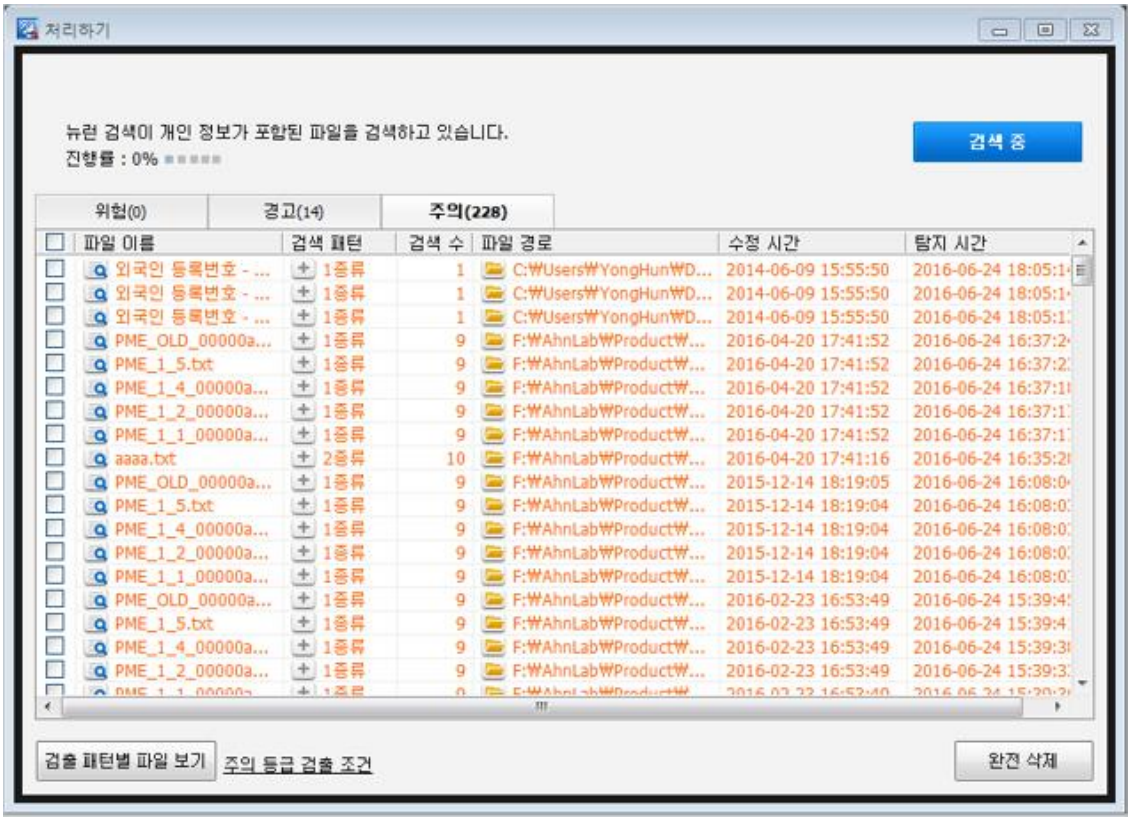
- 안전: PC 에 처리되지 않은 개인 정보 파일 개수가 안전 조건을 초과하지 않았습니다.
- 취약: PC 에 처리되지 않은 개인 정보 파일이 있습니다. **처리하기**를 눌러 PC 내에 처리되지 않은 개인 정보 파일을 처리하십시오.



조치 방법

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

1. 점검 항목 상세 정보에서 **처리하기**를 누릅니다.
2. **처리하기**를 누르면 다음과 같이 개인 정보 검색 창이 실행됩니다.



3. <처리하기>의 **개인 정보 처리 현황**에서 미처리된 파일을 선택하여 **완전 삭제**합니다.

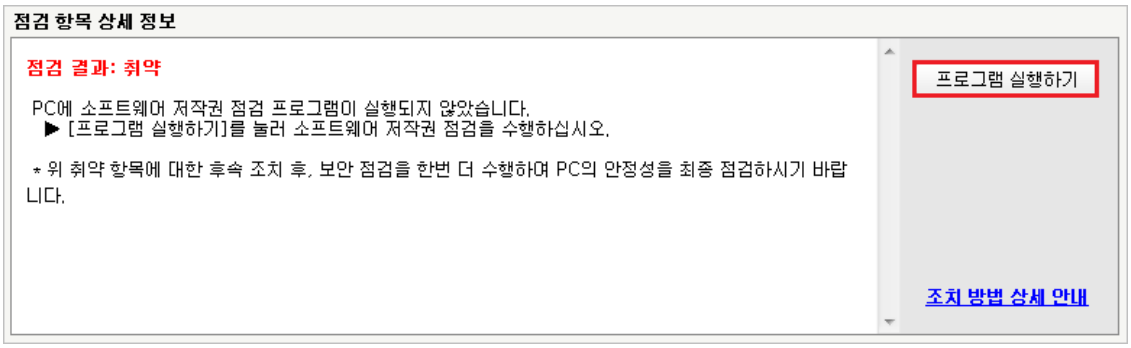
소프트웨어 저작권 점검 프로그램 실행 점검

사용자 PC 에 소프트웨어 저작권 점검 프로그램이 관리자가 지정한 안전 조건 기간 내에 실행되었는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 소프트웨어 저작권 점검 프로그램이 안전 조건 기간 내에 실행되었습니다.
- 취약: PC 에 소프트웨어 저작권 점검 프로그램이 한 번도 실행되지 않았거나, 관리자가 지정한 점검 날짜를 경과하였습니다. **프로그램 실행하기**를 눌러 소프트웨어 저작권 점검을 수행하십시오.

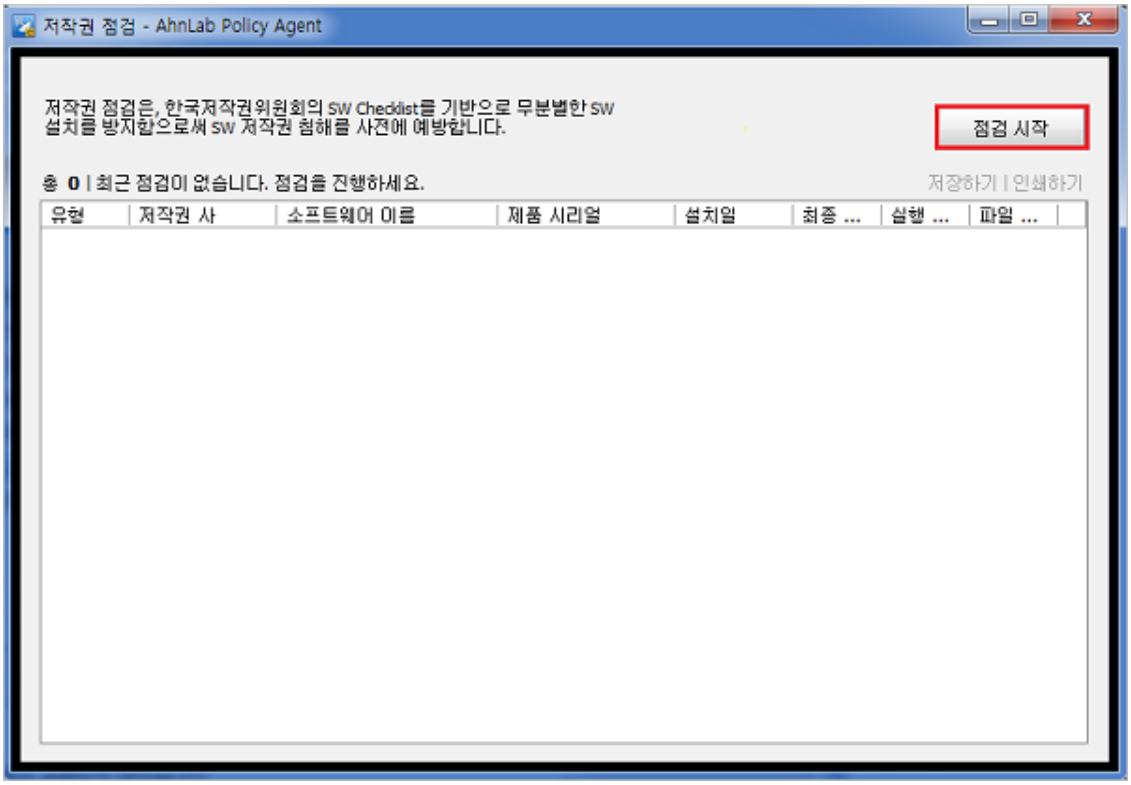


조치 방법

점검 결과가 취약인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

[프로그램 실행하기]

1. 점검 항목 상세 정보에서 **프로그램 실행하기**를 누릅니다.
2. APM 프로그램이 실행되며, <저작권 점검>에서 소프트웨어 저작권 점검 내용을 확인할 수 있습니다.
3. 점검 시작을 눌러 저작권 점검을 진행하십시오.



참고

AhnLab Patch Management 라이선스가 없는 경우에는 점검을 수행할 수 없습니다. 해당 항목을 점검하려면 관련 제품의 라이선스를 구입해야 합니다.

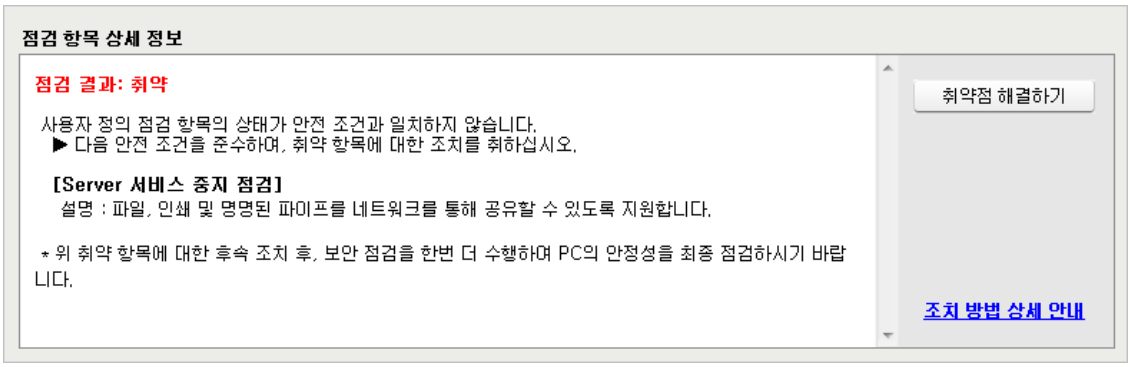
사용자 정의 취약점 점검

사용자 정의 취약점 점검 항목들이 안전 조건을 준수하고 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: 사용자 정의 취약점 점검 항목이 모두 안전 조건을 준수하고 있습니다.
- 취약: 사용자 정의 취약점 점검 결과가 안전 조건을 만족하지 않습니다. 다음의 안전 조건을 준수하여, 취약 항목에 대해 조치하십시오.



조치 방법

점검 결과가 **취약**인 경우, 다음과 같이 조치하여 주시기 바랍니다. 조치 방법은 **서비스 취약**인 경우에만 자동 조치할 수 있습니다.

[서비스 취약]

서비스 취약인 경우, **취약점 해결하기**를 통해 서비스 상태를 변경할 수 있습니다.

1. 점검 항목 상세 정보에서 **취약점 해결하기**를 누릅니다.
2. 관리자가 지정한 안전 조건에 따라 취약 서비스의 상태가 자동으로 변경됩니다.

[사용자 조치]

프로세스 이름, 서비스 이름, 레지스트리 키, 레지스트리 정보, 파일 경로, 파일 버전 취약의 경우 다음과 같이 관리자의 안전 조건을 확인하여 조치해야 합니다.

1. 점검 항목 상세 정보에 명시된 **안전 조건**을 확인합니다.
2. 관리자가 프로세스 이름, 서비스 이름, 레지스트리 키, 레지스트리 정보, 파일 경로, 파일 버전에 대해 지정한 사용자 정의 취약점 안전 조건을 준수하여 관련 항목의 설정을 변경합니다.

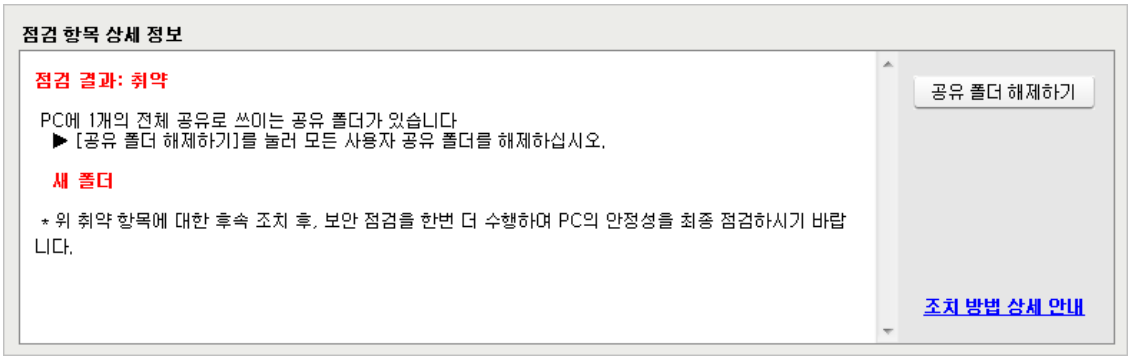
전체 공유(Everyone) 권한의 공유 폴더 사용 점검

Everyone 권한으로 설정되어 있는 공유 폴더를 사용하고 있는지 점검합니다. 최근 악성코드는 공유 폴더를 이용하여 확산되는 경우가 많으므로 공유 폴더는 가능한 사용하지 않는 것이 좋습니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 전체 공유(Everyone) 권한으로 설정된 공유 폴더가 없습니다.
- 취약: PC 에 전체 공유(Everyone) 권한으로 설정된 공유 폴더가 있습니다. **공유 폴더 해제하기**를 눌러 모든 전체 공유 폴더를 해제하십시오.



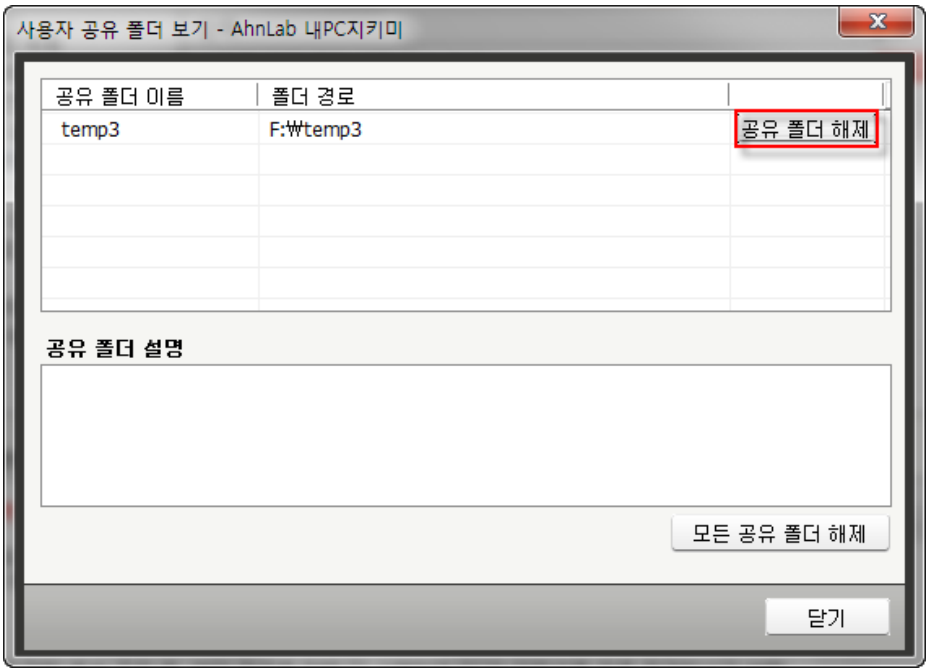
조치 방법

점검 결과가 **취약**인 경우, 다음과 같이 조치하여 주시기 바랍니다.

[공유 폴더 해제하기]

전체 공유로 쓰이는 공유 폴더가 설정되어 있는 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

1. 점검 항목 상세 정보에서 **공유 폴더 해제하기**를 누릅니다.
2. 공유 폴더 목록이 표시됩니다.



- 공유 폴더 해제: 선택한 폴더의 공유를 해제합니다.
- 모든 공유 폴더 해제: 설정되어 있는 모든 공유 폴더의 공유를 해제합니다.

3. **공유 폴더 해제** 또는 **모든 공유 폴더 해제**를 누르면 설정되어 있는 공유 폴더가 해제됩니다.

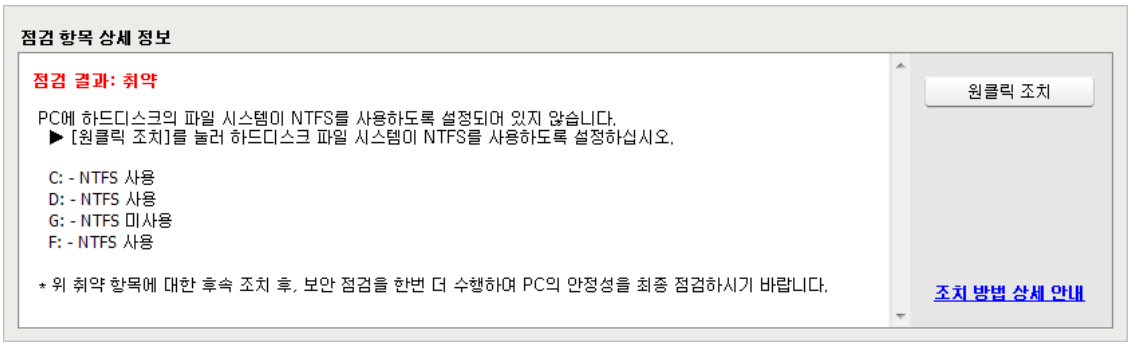
하드디스크 파일 시스템의 NTFS 사용 점검

사용자 PC 에 하드디스크 파일 시스템이 NTFS 를 사용하도록 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 의 하드디스크 파일 시스템이 NTFS 입니다.
- 취약: PC 에 하드디스크의 파일 시스템이 NTFS 를 사용하도록 설정되어 있지 않습니다. **설정하기**를 눌러 하드디스크 파일 시스템이 NTFS 를 사용하도록 설정하십시오.

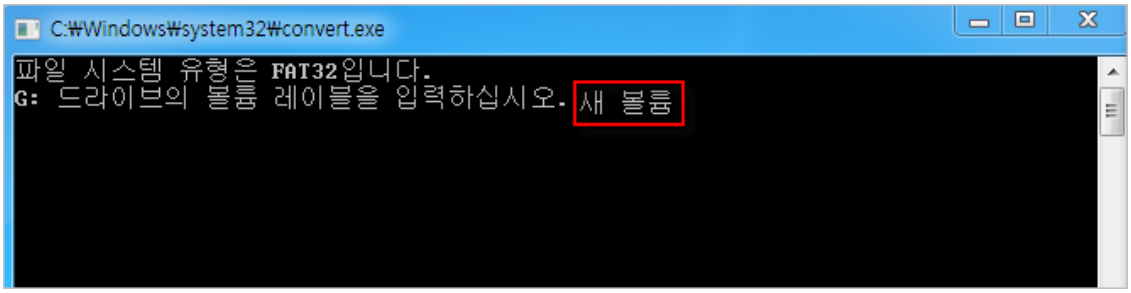


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. **원클릭 조치**를 눌러 하드디스크의 파일 시스템이 NTFS 를 사용하도록 설정하면 다음과 같은 커맨드 창이 나타납니다. NTFS 변경되는 볼륨의 레이블을 입력합니다.
   - 입력 예) 드라이브의 볼륨 레이블이 **새 볼륨(G:)**라면 **새 볼륨**을 입력합니다.



3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

점검 결과가 취약인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

1. **점검 항목 상세 정보**에서 현재 PC의 하드디스크 파일 시스템의 NTFS 사용 현황을 파악합니다.
2. **시작** > **실행**을 클릭하여, **cmd**를 입력한 다음 **확인**을 누릅니다.
3. <명령 프롬프트>가 실행되면 다음과 같은 명령어를 입력합니다.

```
CONVERT 변경할 하드디스크 문자: /FS:NTFS
```

- 예시: CONVERT D: /FS:NTFS

4. Convert.exe가 실행되어 하드디스크의 파일 시스템을 NTFS로 변환합니다.

주의

하드디스크의 파일 시스템 변환은 단 방향으로만 수행됩니다. 따라서 파일 시스템을 NTFS 로 변환한 후에는 다시 FAT 로 변환할 수 없습니다.

참고

파일 시스템을 변환 시켜주는 Convert.exe 는 Windows XP 이상의 운영체제부터 지원되므로 본 조치 방법은 Windows XP 이상 환경에서 참고하시기 바랍니다.

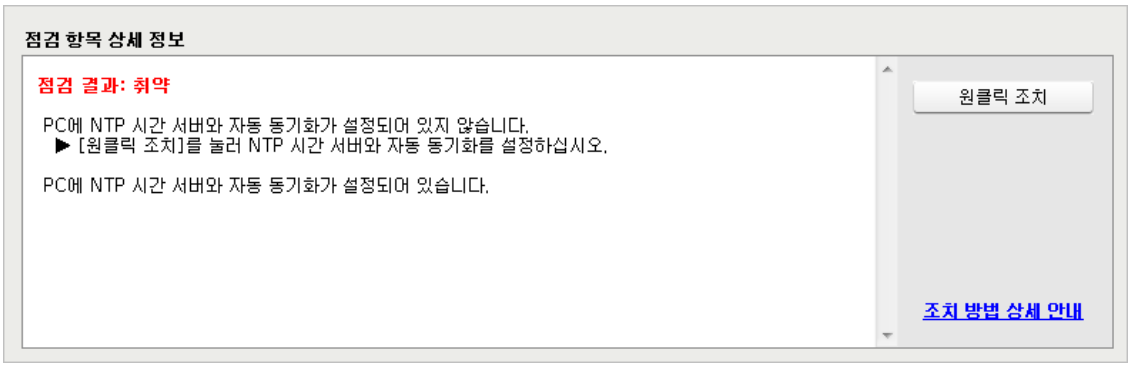
NTP 시간 서버와 자동 동기화 설정 점검

사용자 PC 의 시간이 NTP 시간 서버와 자동 동기화되도록 설정되어 있는지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: PC 에 NTP 시간 서버와 자동 동기화가 설정되어 있습니다.
- 취약: PC 에 NTP 시간 서버와 자동 동기화가 설정되어 있지 않습니다. **원클릭 조치**를 눌러 NTP 시간 서버와 자동 동기화를 설정하십시오.

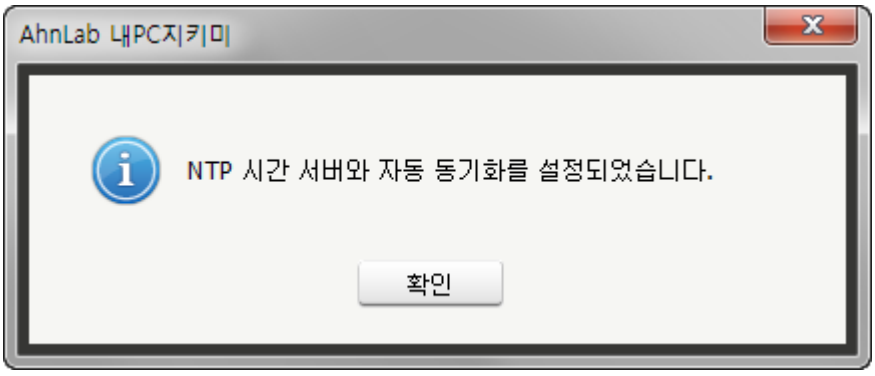


조치 방법

조치 방법에는 원클릭 조치 버튼을 통한 조치와 사용자가 직접 조치할 수 있는 사용자 조치 방법이 있습니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. NTP 시간 서버와 자동 동기화가 설정하면 다음과 같은 알림 창이 나타납니다.

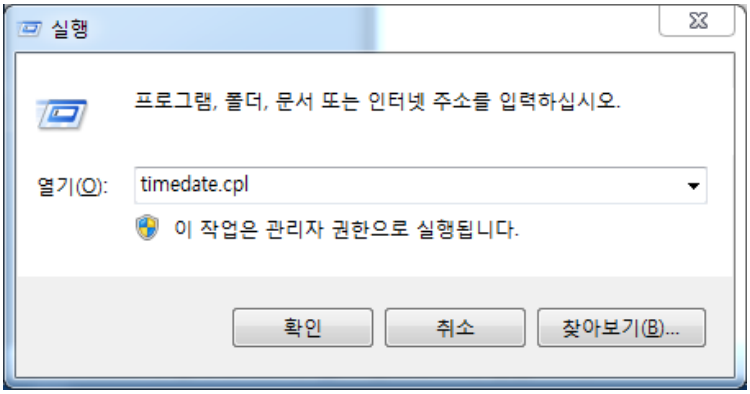


3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

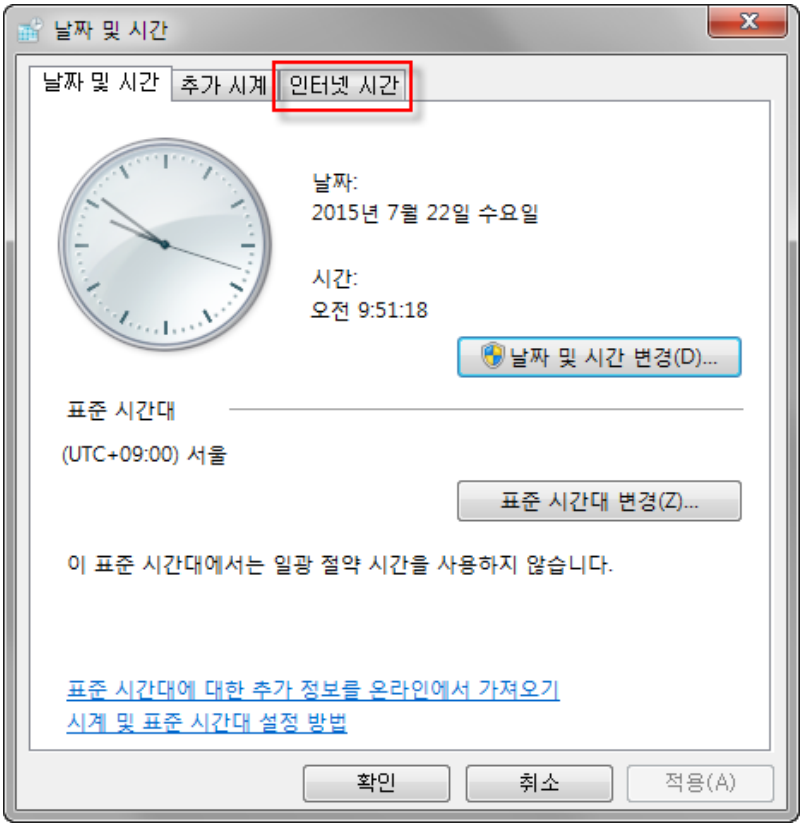
[사용자 조치]

시간이 자동으로 동기화되고 있지 않은 경우 다음과 같은 방법을 통하여 조치할 수 있습니다.

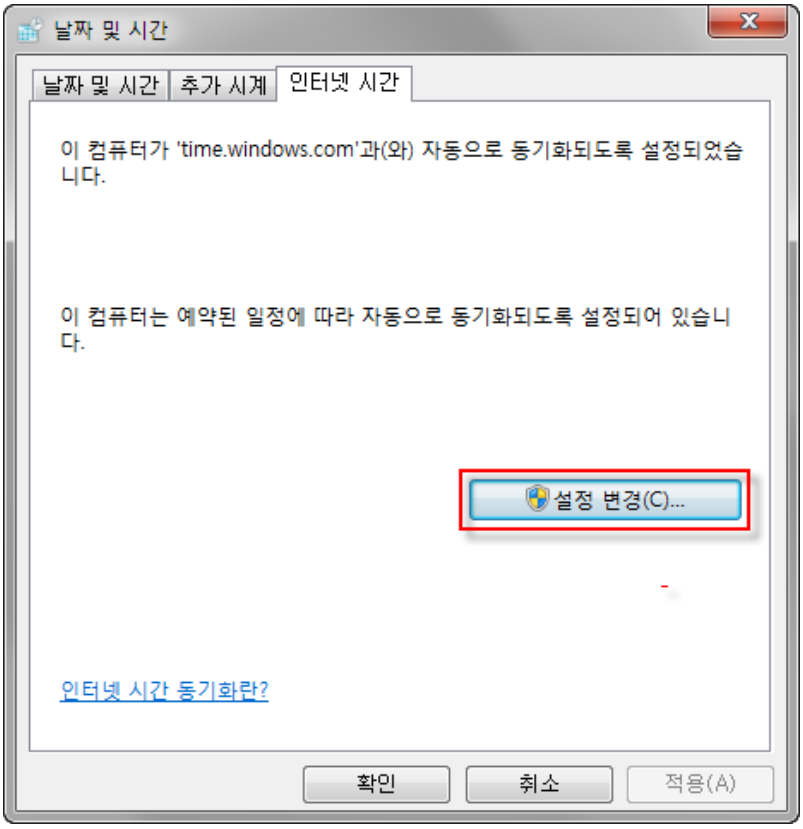
1. 윈도우 + R키를 눌러 실행 창을 띄운 후 **timedate.cpl**를 입력합니다.



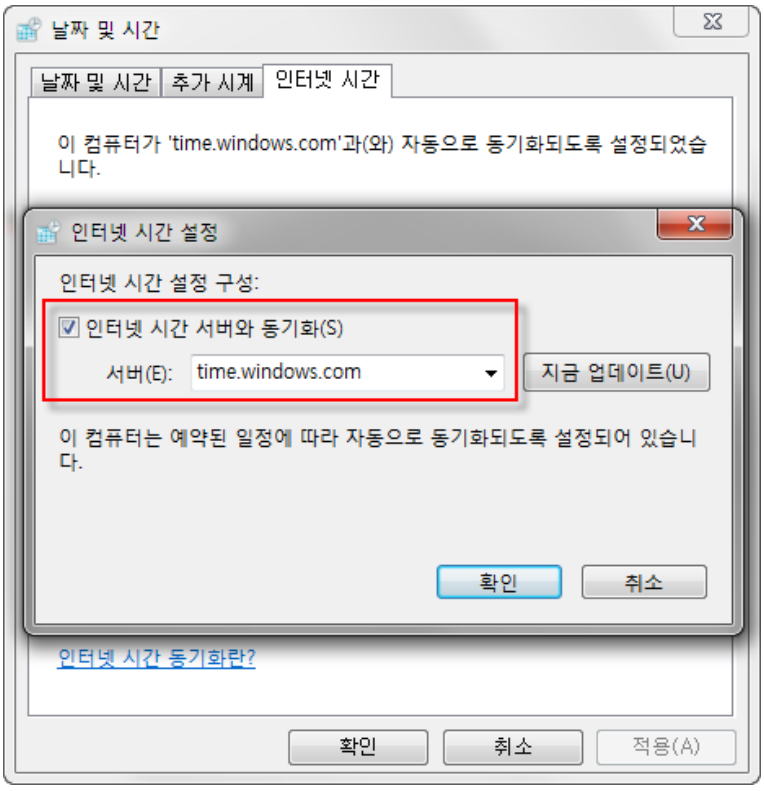
2. 우측 상단의 **인터넷 시간** 탭을 클릭합니다.



3. **설정 변경**을 클릭합니다.



4. **인터넷 시간 서버와 동기화**를 체크 후 서버에 **time.windows.com** 또는 조직 내 **지정된 NTP 시간 서버의 주소**를 입력한 후 **확인**을 클릭하여 설정을 종료합니다.



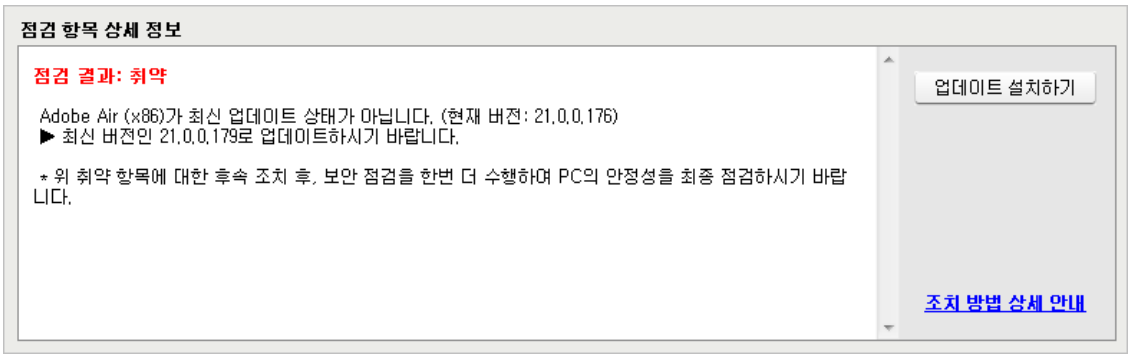
Adobe AIR 최신 업데이트 점검

Adobe AIR 가 최신으로 업데이트되어 있는 지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: Adobe Air 가 최신으로 업데이트되어 있습니다.
- 취약: Adobe Air 가 최신 업데이트 상태가 아닙니다. **업데이트 설치하기**를 눌러 최신 버전의 보안 업데이트를 설치하십시오.



조치 방법

점검 결과가 **취약**일 때, APM 라이선스가 없는 경우와 APM 라이선스가 있는 경우에 따라 다음과 같이 조치하여 주시기 바랍니다.

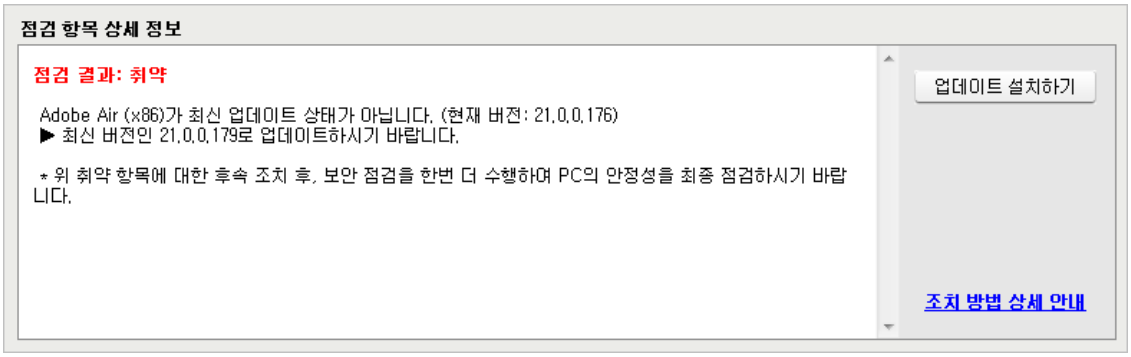
[APM 라이선스가 없는 경우]

1. 점검 항목 상세 정보에서 **업데이트 설치하기**를 누릅니다.
2. Adobe 홈페이지에서 최신 파일을 다운로드 하여 설치합니다.

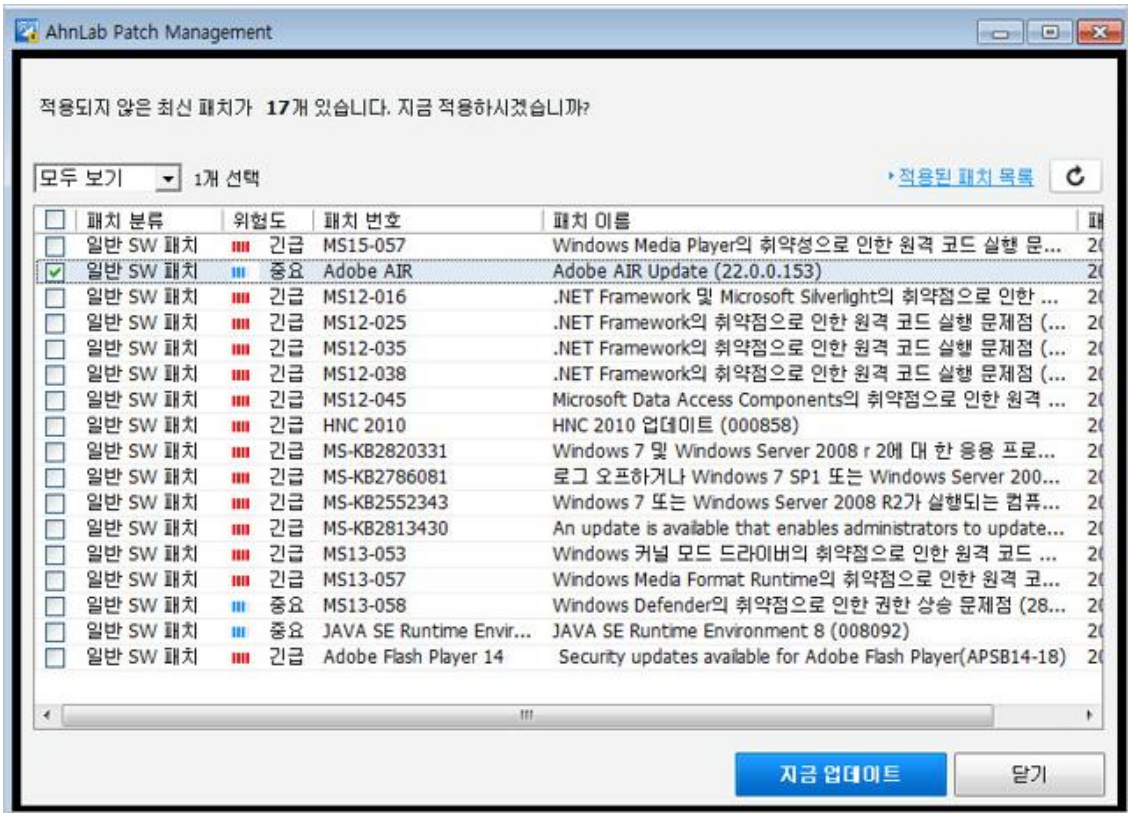
[APM 라이선스가 있는 경우]

APM 제품을 통해 적용되지 않은 패치 목록을 확인하고 최신 보안 패치를 적용할 수 있습니다.

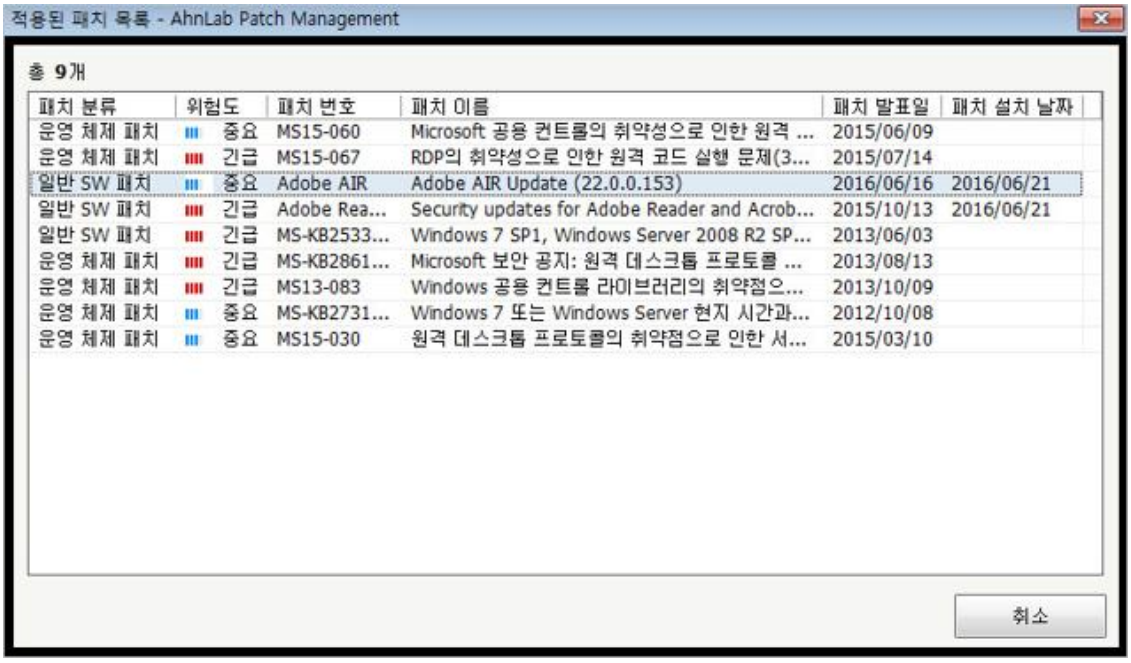
1. 업데이트 설치하기를 누릅니다.



2. APM이 실행되며 <패치 정보 보기>에서 현재 사용자 PC에 적용되지 않은 패치 목록을 확인할 수 있습니다.



3. **지금 업데이트**를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.
4. 패치 적용이 완료되면 화면 상단의 **적용된 패치 목록**을 눌러 설치된 패치 정보를 확인할 수 있습니다.



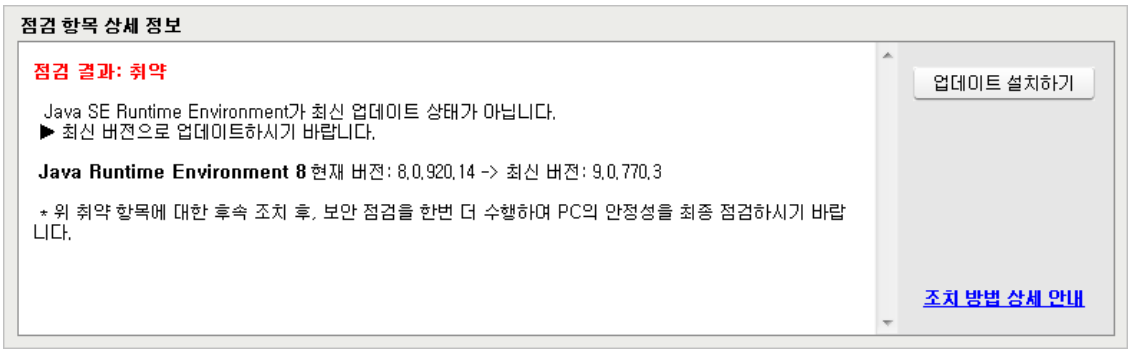
Java SE Runtime Environment 최신 업데이트 점검

Java SE Runtime Environment 가 최신으로 업데이트되어 있는 지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: Java SE Runtime Environment 가 최신으로 업데이트되어 있습니다.
- 취약: Java SE Runtime Environment 가 최신 업데이트 상태가 아닙니다. **업데이트 설치하기**를 눌러 최신 버전의 보안 업데이트를 설치하십시오.



조치 방법

점검 결과가 **취약**일 때, APM 라이선스가 없는 경우와 APM 라이선스가 있는 경우에 따라 다음과 같이 조치하여 주시기 바랍니다.

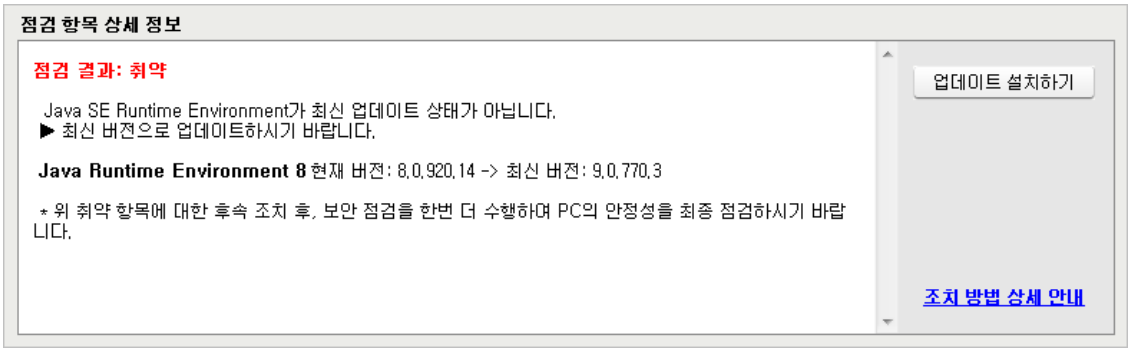
[APM 라이선스가 없는 경우]

1. 점검 항목 상세 정보에서 **업데이트 설치하기**를 누릅니다.
2. Oracle 홈페이지에서 최신 파일을 다운로드 하여 설치합니다.

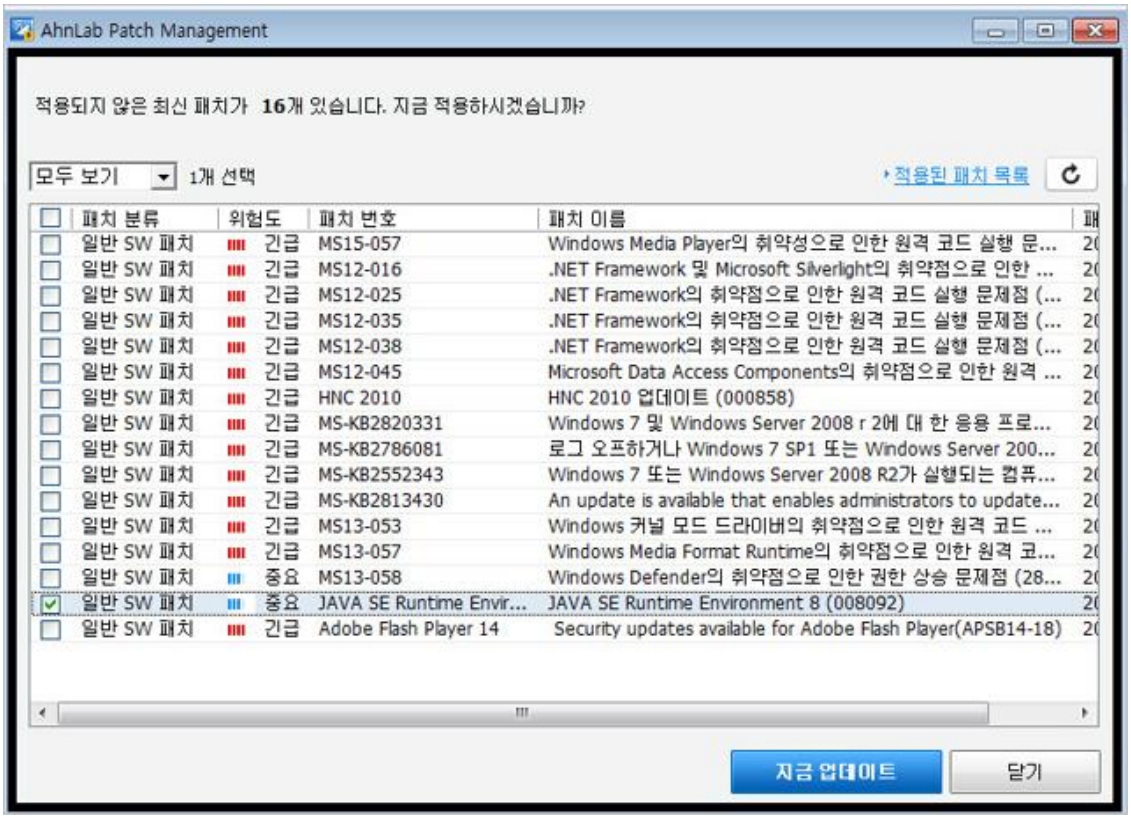
[APM 라이선스가 있는 경우]

APM 제품을 통해 적용되지 않은 패치 목록을 확인하고 최신 보안 패치를 적용할 수 있습니다.

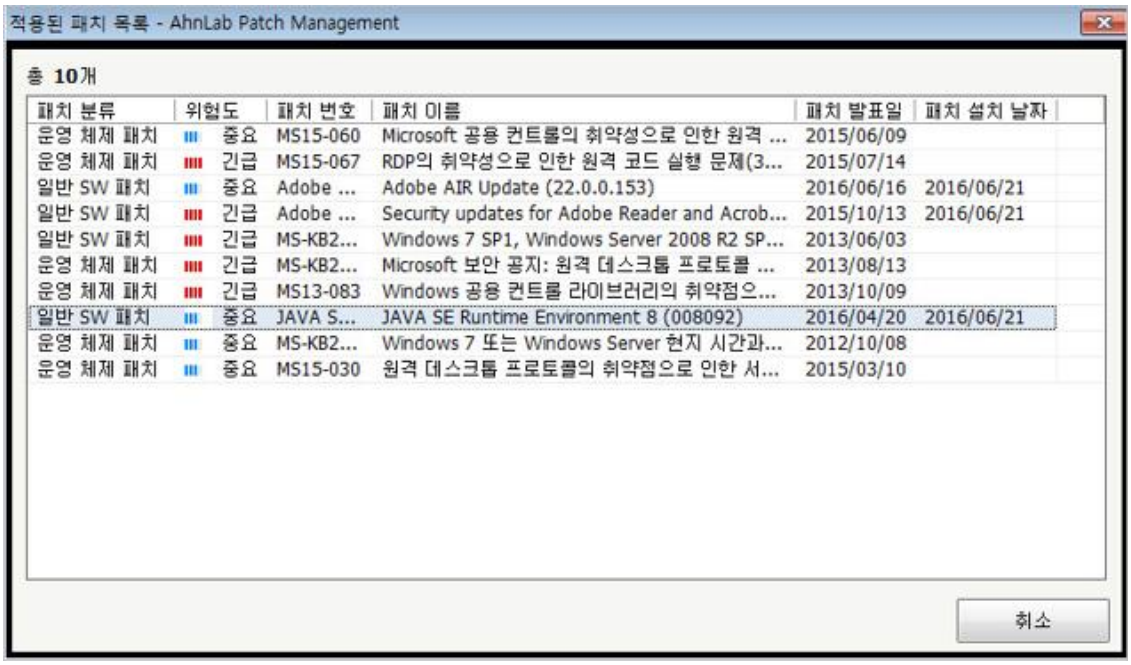
1. 업데이트 설치하기를 누릅니다.



2. APM이 실행되며 <패치 정보 보기>에서 현재 사용자 PC에 적용되지 않은 패치 목록을 확인할 수 있습니다.



3. **지금 업데이트**를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.
4. 패치 적용이 완료되면 화면 상단의 **적용된 패치 목록**을 눌러 설치된 패치 정보를 확인할 수 있습니다.



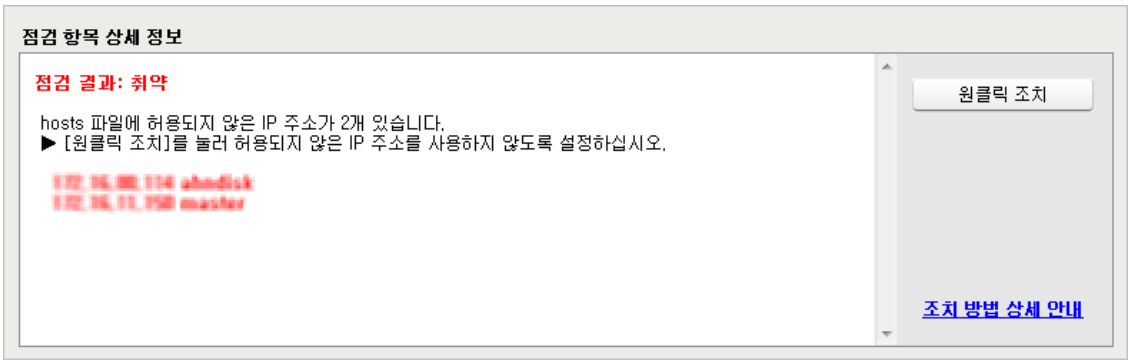
hosts 파일 내 비허용 IP 점검

hosts 파일에 허용되지 않은 IP 주소가 설정되어 있는 지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: hosts 파일에 허용되지 않은 IP 주소가 존재하지 않습니다.
- 취약: hosts 파일에 허용되지 않은 IP 주소가 있습니다. **원클릭 조치**를 눌러 허용되지 않은 IP 주소를 사용하지 않도록 설정하십시오.



조치 방법

조치 방법에는 원클릭 조치 버튼을 통해 조치할 수 있습니다.

[원클릭 조치]

1. 점검 항목 상세 정보에서 **원클릭 조치**를 누릅니다.
2. 허용되지 않은 IP 주소를 사용하지 않도록 설정하면 다음과 같은 알림 창이 나타납니다.
3. 알림 창에서 **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

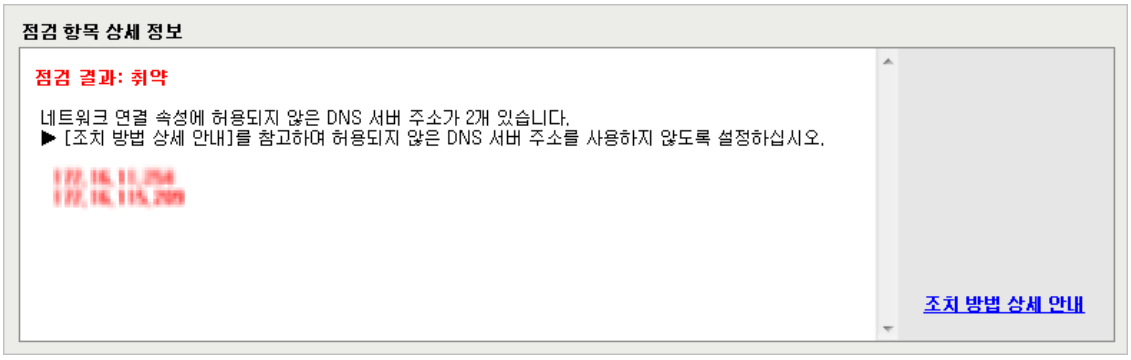
비허용 DNS 설정 점검

네트워크 연결 속성에 허용되지 않은 DNS 서버 주소가 설정되어 있는 지 점검합니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: 네트워크 연결 속성에 허용되지 않은 DNS 서버 주소가 존재하지 않습니다.
- 취약: 네트워크 연결 속성에 허용되지 않은 DNS 서버 주소가 있습니다. **조치 방법 상세 안내**를 참고하여 허용되지 않은 DNS 서버 주소를 사용하지 않도록 설정하십시오.



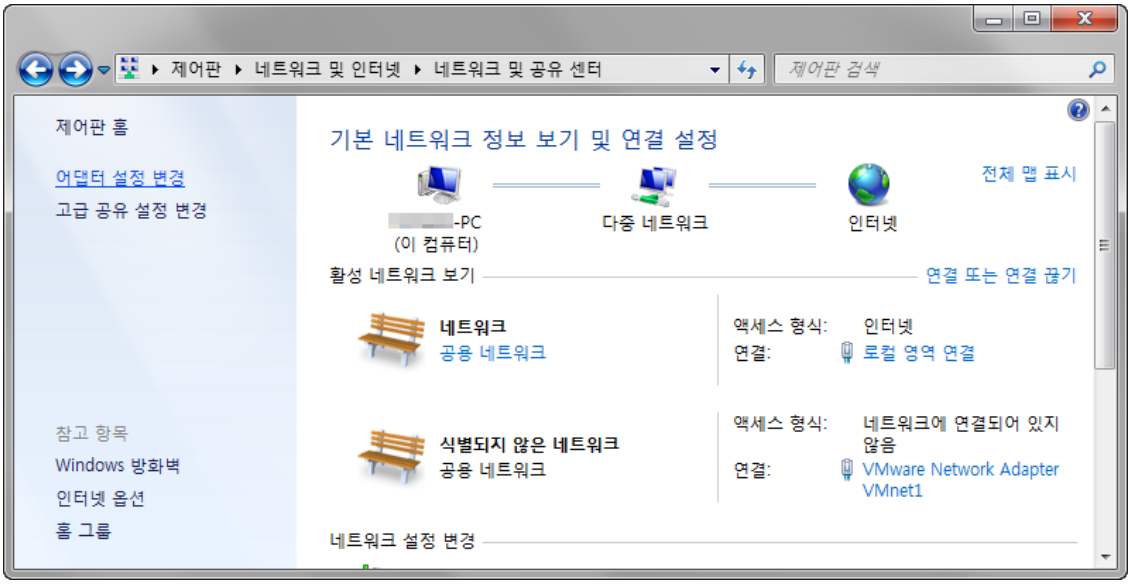
조치 방법

점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

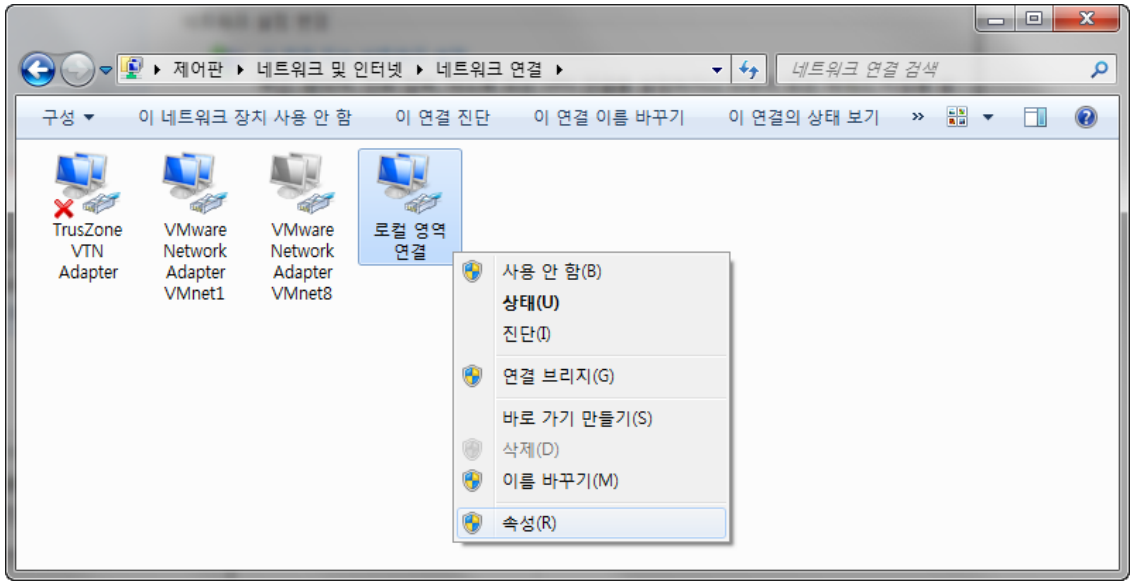
[사용자 조치]

비허용 DNS 가 설정된 경우 다음과 같은 방법으로 설정을 해제합니다.

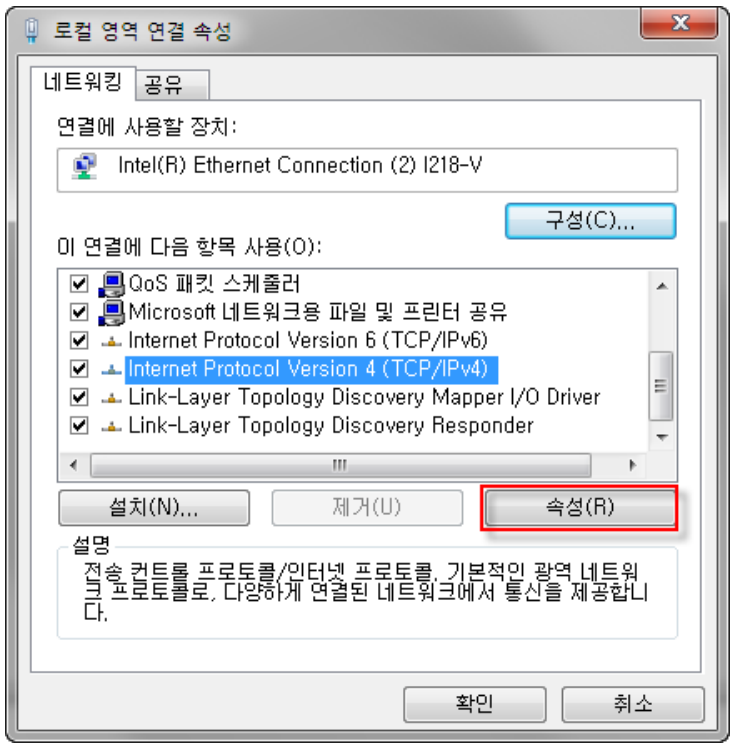
1. 제어판에서 **제어판> 네트워크 및 인터넷 > 네트워크 및 공유 센터**로 이동합니다.
2. <네트워크 및 공유 센터>에서 **어댑터 설정 변경**을 누릅니다.



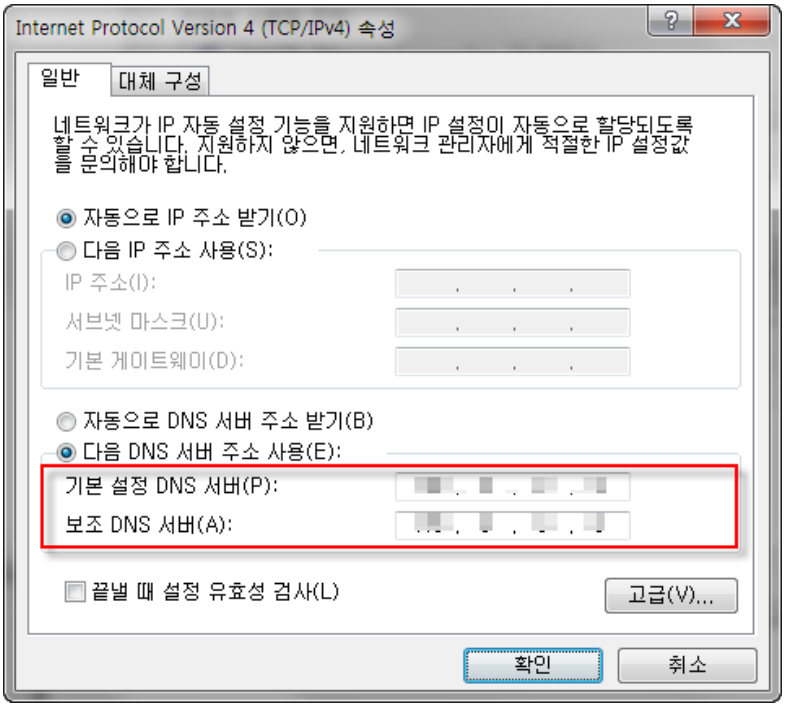
3. 로컬 영역 연결 아이콘을 마우스 오른쪽으로 눌러 **속성** 메뉴를 선택합니다.



4. <로컬 영역 연결 속성>의 네트워킹 탭에서 **Internet Protocol Version 4(TCP/IPv4)**를 선택하고, **속성**을 누릅니다.



5. <**Internet Protocol Version 4(TCP/IPv4) 속성**>에서 기본 설정 DNS 서버와 보조 DNS 서버의 IP 를 확인합니다.



- 설정된 DNS 정보가 관리자 지정한 허용 IP 가 아니면, 관리자가 지정한 IP 정보로 변경합니다.

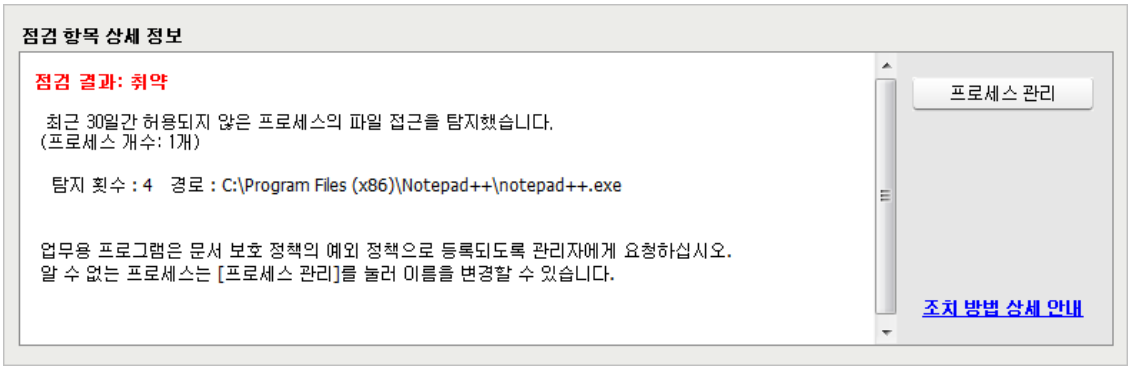
문서 보호 기능 점검

특정 문서 확장자(doc, docx, ...)를 가진 파일에 대해 허용된 프로세스만 접근을 허용하고, 나머지 프로세스는 모두 접근을 차단하여 문서를 보호하는 기능 입니다.

점검 결과

점검 항목 상세 정보에서는 다음과 같이 안전, 취약에 대한 점검 결과를 나타냅니다.

- 안전: 허용되지 않은 프로세스의 접근 기록이 없습니다.
- 취약: 최근 몇 일 동안 허용되지 않은 프로세스가 파일에 접근하는 것을 탐지했습니다. 업무용 프로그램은 문서 보호 정책의 예외 정책으로 등록되도록 관리자에게 요청하십시오. 알 수 없는 프로세스는 **프로세스 관리**를 눌러 이름을 변경할 수 있습니다.

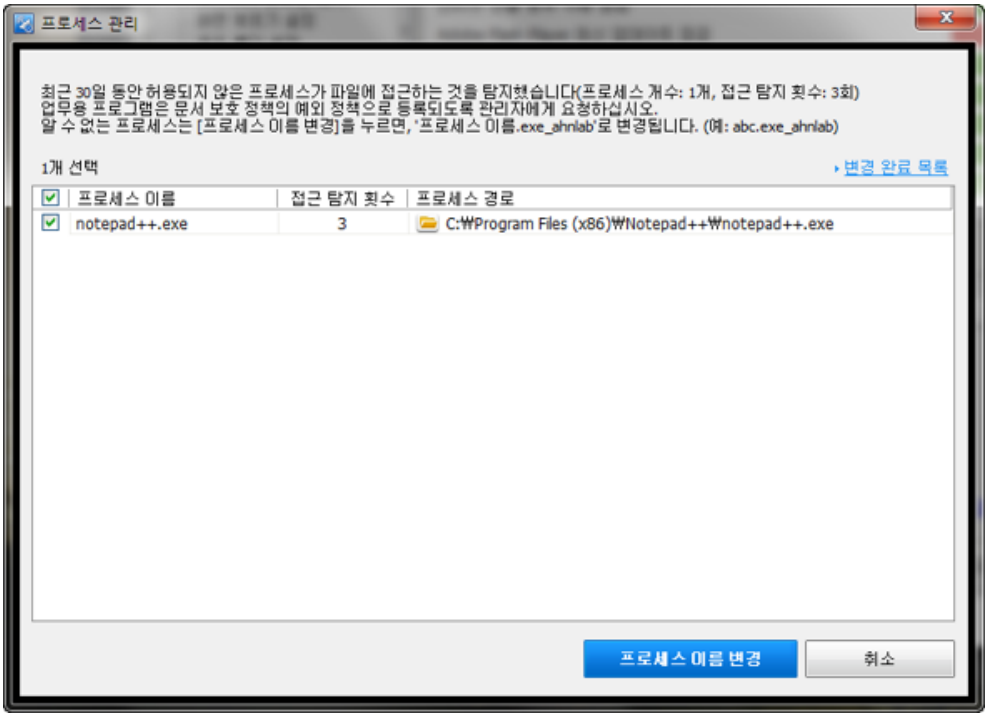


조치 방법

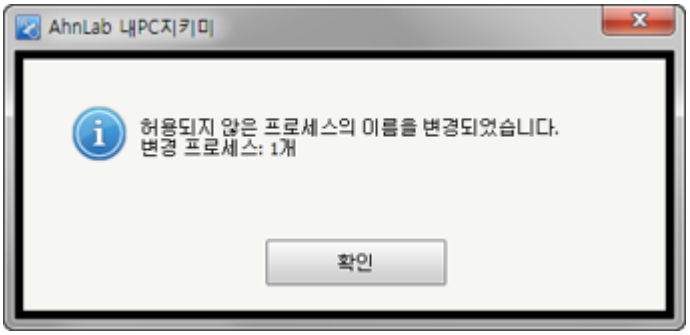
점검 결과가 **취약**인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

[프로세스 관리]

1. 점검 항목 상세 정보에서 **프로세스 관리**를 누릅니다.



2. <프로세스 관리>에서 변경을 원하는 프로세스를 선택한 뒤, **프로세스 이름 변경**을 누릅니다.
3. 프로세스 이름 변경이 완료되면 다음과 같은 알림 창이 발생합니다.



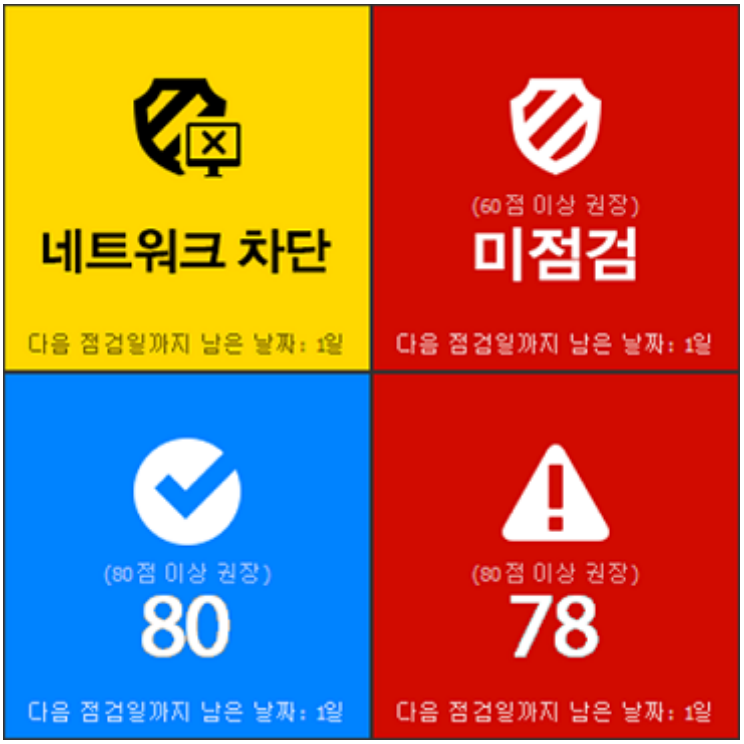
4. **확인**을 누르면 점검 결과는 안전으로 변경됩니다.

9 장

위젯

위젯 기능

위젯을 통해 바탕화면에서 내 PC 지키미 에이전트의 기본 정보를 확인하고, 사용자 PC 의 상태를 파악할 수 있습니다.



에이전트 상태 표시

- 네트워크 차단 상태: 특정 항목의 점검 결과가 취약으로 판단되어, 네트워크가 차단된 경우입니다.
- 미점검 상태: 사용자 PC 에서 한번도 내 PC 지키미 점검을 수행하지 않은 경우입니다. 위젯을 더블클릭하면 AhnLab 내 PC 지키미 화면이 실행됩니다.
- 안전 상태: 설정 보안 점수보다 높을 경우, 안전 상태로 표시합니다.
- 취약 상태: 설정 보안 점수보다 낮을 경우, 취약 상태로 표시합니다.

점검 상태 표시

- 점검 점수: 사용자 PC 에서 1 회 이상 점검을 수행한 경우, 위젯에 점검 점수를 표시합니다.
- 안전 상태: 파란색으로 표시되며, 기준 점수와 같거나 높은 경우입니다.
- 취약 상태: 빨간색으로 표시되며, 기준 점수보다 낮은 경우입니다.
- 다음 점검일: 다음 점검일까지 남은 날짜를 표시합니다.

참고

위젯 기능은 관리자가 내 PC 지키미 기본 정책으로 위젯을 사용하도록 설정한 경우에만 작동합니다.

10 장

작업 표시줄

사용자 정보

작업 표시줄에 있는 Policy Agent 의 아이콘()을 누르면, 사용자 정보를 에이전트 사용자가 직접 입력할 수 있습니다. 입력한 사용자 정보는 Policy Server 로 전송되어 서버 관리자가 해당 에이전트의 사용자 정보를 확인할 수 있습니다.

1. 작업 표시줄의 에이전트 아이콘()에서 마우스 오른쪽을 눌러 **사용자 정보**를 선택합니다.
2. <사용자 정보>가 나타나면 항목을 입력합니다.
    - 사원 이름: 에이전트 사용자의 실명을 입력합니다.
    - 소속 부서: 소속 부서의 이름을 입력합니다.
    - 전화 번호: 회사 내선 전화 번호나 이동 전화 번호를 입력합니다.
    - 메일 주소: 메일 주소를 입력합니다.
- 사원 번호: 사원 번호를 입력합니다.

 **참고**

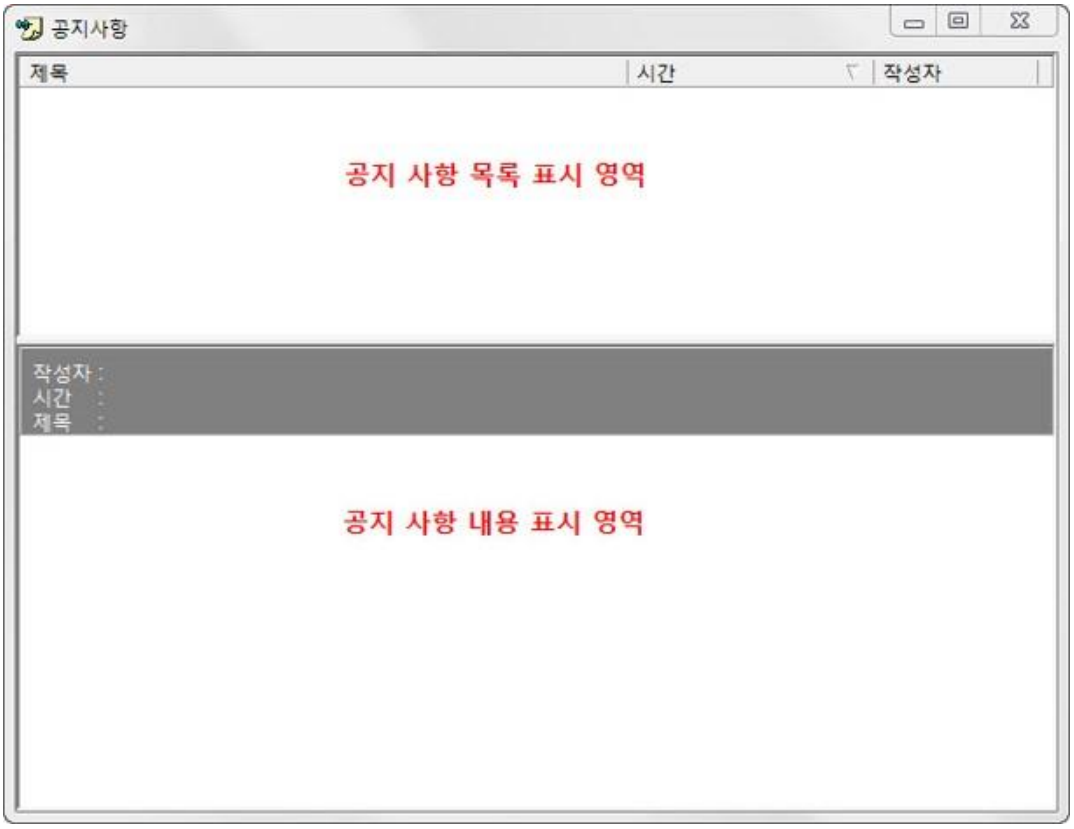
모든 입력 항목은 Policy Server 관리자의 안내에 따라 입력하십시오. 관리자의 안내에 따라 요구하는 방법대로 항목을 입력하시기 바랍니다.

3. **확인**을 누릅니다.

공지사항 보기

서버 관리자가 작성한 공지사항을 볼 수 있습니다. 공지사항이 에이전트에 도착하면, 팝업으로 내용이 나타납니다. 팝업으로 즉시 공지사항을 확인하거나 작업 표시줄의 에이전트 아이콘을 눌러 공지사항을 확인할 수도 있습니다.

1. 작업 표시줄의 내 PC 지키미 아이콘( )에서 마우스 오른쪽을 눌러 **공지 사항 보기**를 선택합니다.
2. <공지사항>이 나타나면 내용을 확인합니다. 공지사항의 윗부분은 관리자가 보낸 공지사항 목록이며, 아래 부분은 목록에서 선택한 공지사항의 내용이 보입니다.



고급 설정

Policy Server 와 통신을 위해 에이전트의 네트워크 환경을 설정할 수 있습니다. 에이전트 설치 파일을 만들 때 서버 관리자가 NAT 환경에 따른 설정을 해서 배포하여 설치한 경우 고급 설정에서 직접 NAT 환경에 따른 네트워크 설정을 할 필요는 없습니다. 고급 설정의 네트워크 환경 설정은 서버 관리자에게 문의하신 후에 관리자의 안내에 따라 설정을 하시기 바랍니다.

1. 작업 표시줄의 에이전트 아이콘( )에서 마우스 오른쪽을 눌러 **기타 옵션** > **고급 설정**을 선택합니다.
2. <고급 설정>이 나타납니다.
   - Policy Server 가 NAT 안에 있는 경우: Policy Server 가 NAT 안에 있는 경우 Policy Server 가 사설 IP 주소를 가지므로 에이전트에서 Policy Server 로 연결할 수 없습니다. 이러한 경우 Policy Server 의 네트워크 포트를 2 개 이상으로 구성하여 에이전트와 통신합니다.
     - Policy Server 사설 IP 주소: Policy Server 의 사설 IP 주소를 입력합니다.
     - Policy Server 공인 IP 주소: Policy Server 의 공인 IP 주소를 입력합니다. Policy Server 의 공인 IP 주소와 에이전트의 IP 주소는 서로 같은 네트워크에 있어야 합니다.
     - 연결 테스트: 네트워크 설정대로 Policy Server 와 통신이 가능한지 확인합니다.
3. **확인**을 누릅니다.

제품 정보

사용 중인 에이전트의 버전 정보를 확인하고 접속 중인 Policy Server 의 IP 주소를 확인할 수 있습니다.

1. 작업 표시줄의 에이전트 아이콘()에서 마우스 오른쪽을 눌러 **제품 정보**를 선택합니다.
2. <제품 정보>가 나타납니다.
   - 서버 IP 주소: 에이전트가 접속 중인 Policy Server 의 IP 주소를 보여줍니다.
   - 로컬 IP 주소: 에이전트를 설치한 PC 의 IP 주소를 보여줍니다.

11 장

자주하는 질문(FAQ)

Q1. 바이러스 백신이 설치/실행되고 있는데도 바이러스 백신 설치 및 실행 점검이 '취약'으로 표시됩니다.

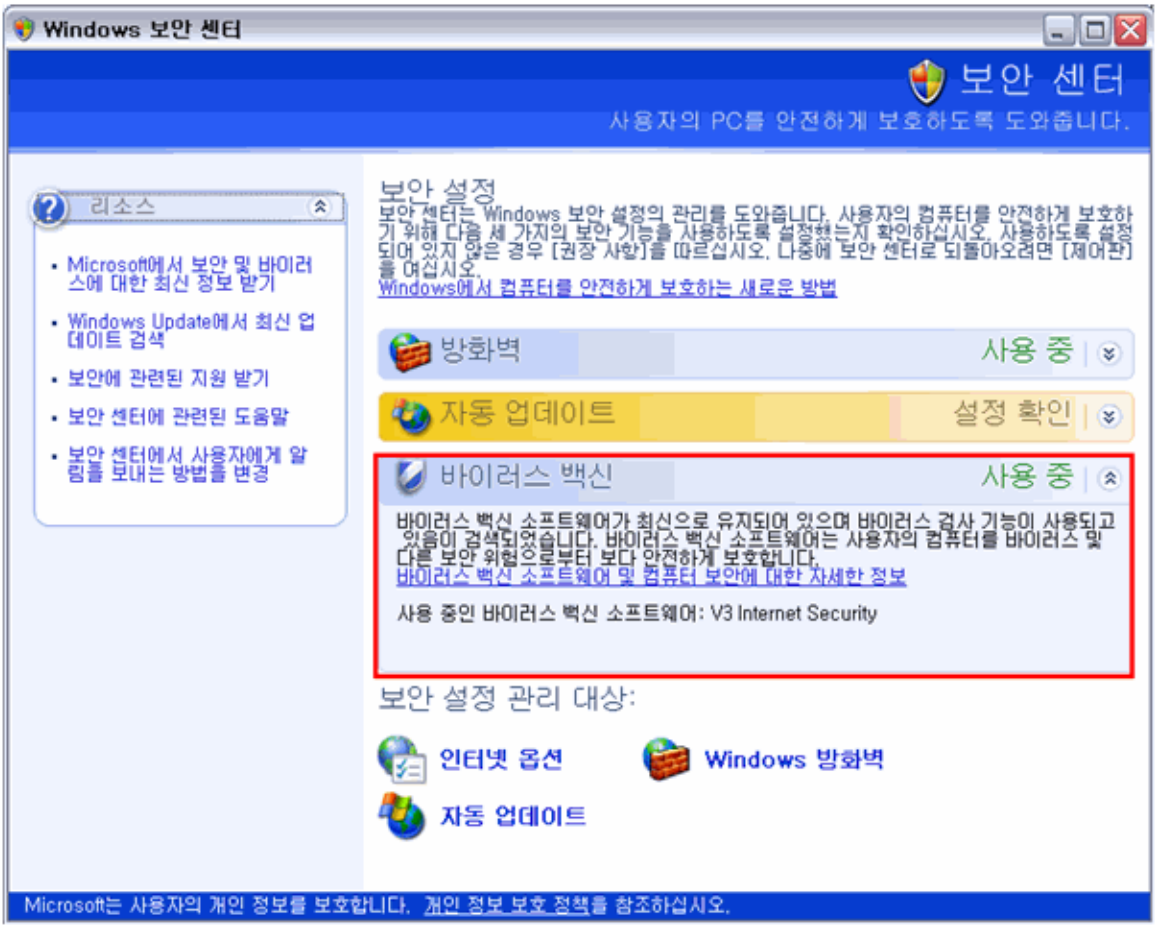
사용 중인 Windows 운영체제에 맞는 내 PC 지키미를 설치하십시오. Windows Vista 나 Windows 7 의 경우 내 PC 지키미 버전이 권장 버전 보다 낮은 경우 점검 결과가 다르게 표시될 수 있습니다.

참고

바이러스 백신 설치 및 실행 점검은 제어판의 보안 센터에 등록된 백신 정보를 기반으로 점검합니다.

보안 센터에서 바이러스 백신 정보 확인하기

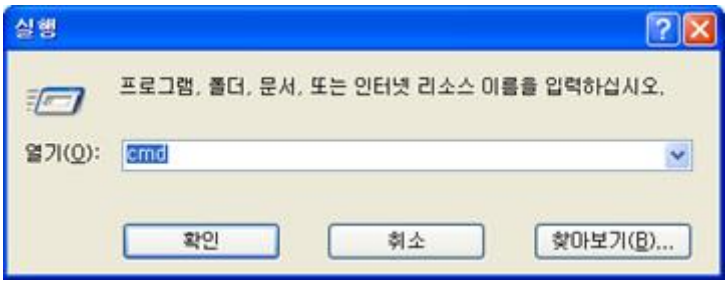
보안 센터는 Windows XP SP2 이상에서만 사용할 수 있으므로 사용 중인 PC 의 Windows XP 라면 서비스 팩 2 이상인지 확인합니다.



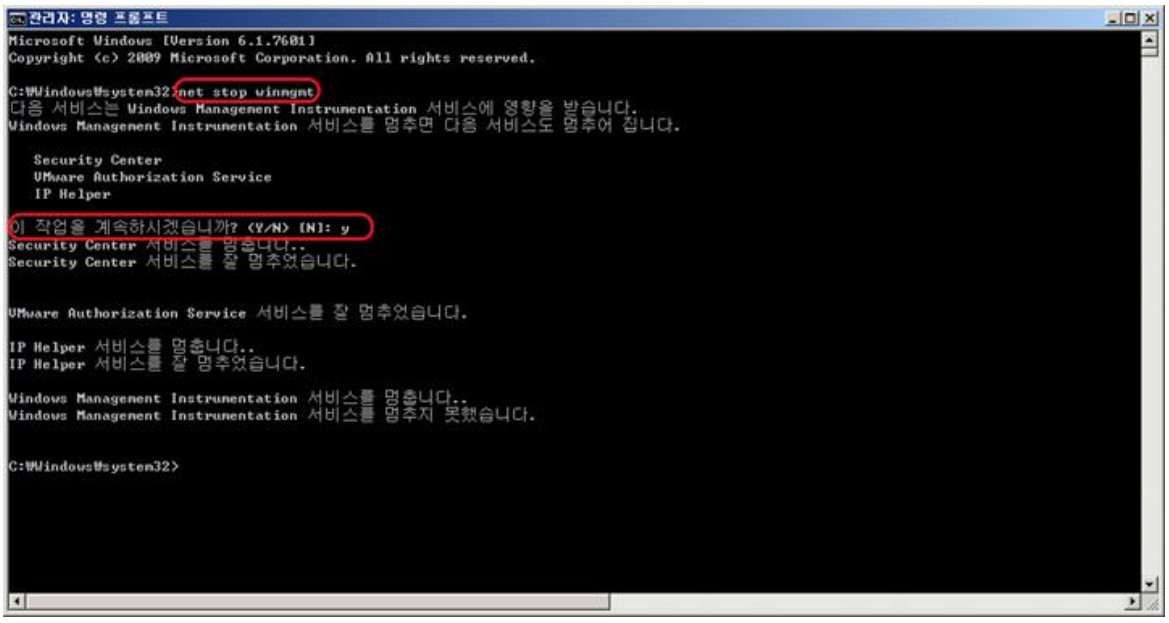
- 서비스 팩 2 이상인 경우 보안 센터에서 사용 중인 백신 제품의 정보가 표시되고 **사용 중**으로 표시되는지 확인하십시오.
- 바이러스백신 정보가 찾을 수 없음이나 사용 안 함으로 표시되면 점검 결과는 취약으로 표시됩니다.
- 백신이 설치되어 있는 경우에 보안 센터에 해당 정보가 표시되지 않는 이유: 설치된 백신 제품에서 Windows 보안 센터에 정보를 제공하지 않거나 설치 정보가 일치하지 않기 때문입니다.
- 보안 센터에서 바이러스 백신 정보가 사용 중으로 표시되지만 점검 결과가 취약인 경우: **시스템 보안 정보 집합체**를 재설정하십시오.

시스템 보안정보 집합체 재설정 하는 방법

1. **시작** > **실행**을 누른 후 입력 창에 **cmd**를 입력합니다.

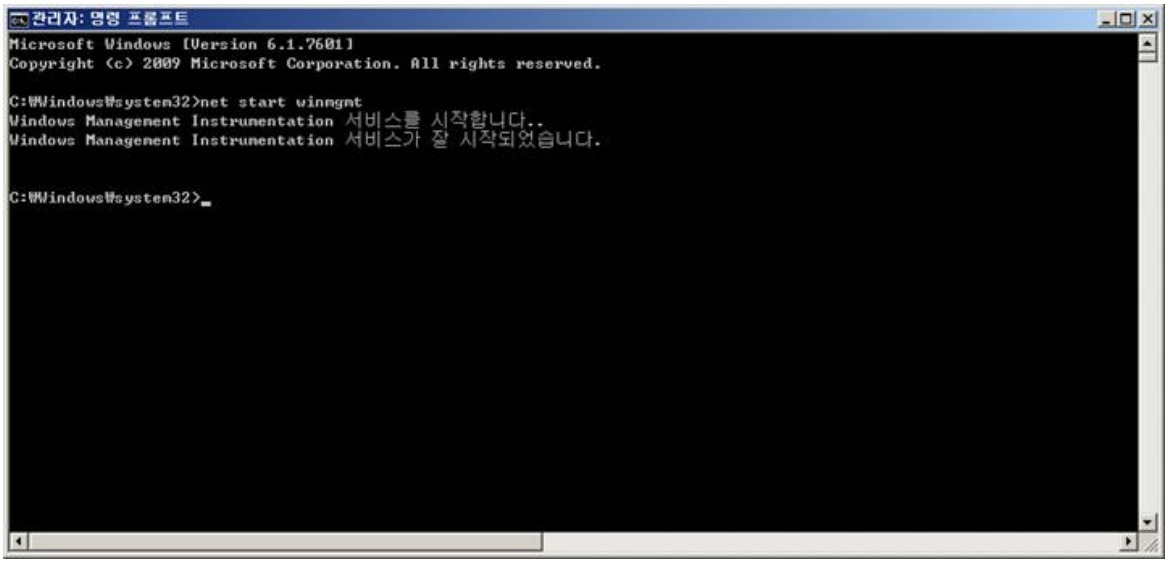


2. 명령어 창에 **net stop winmgmt**를 입력합니다. ***서비스를 멈추면 다음 서비스도 멈추어집니다. 이 작업을 계속 하시겠습니까?** 라는 메시지에 **Y**를 입력합니다.

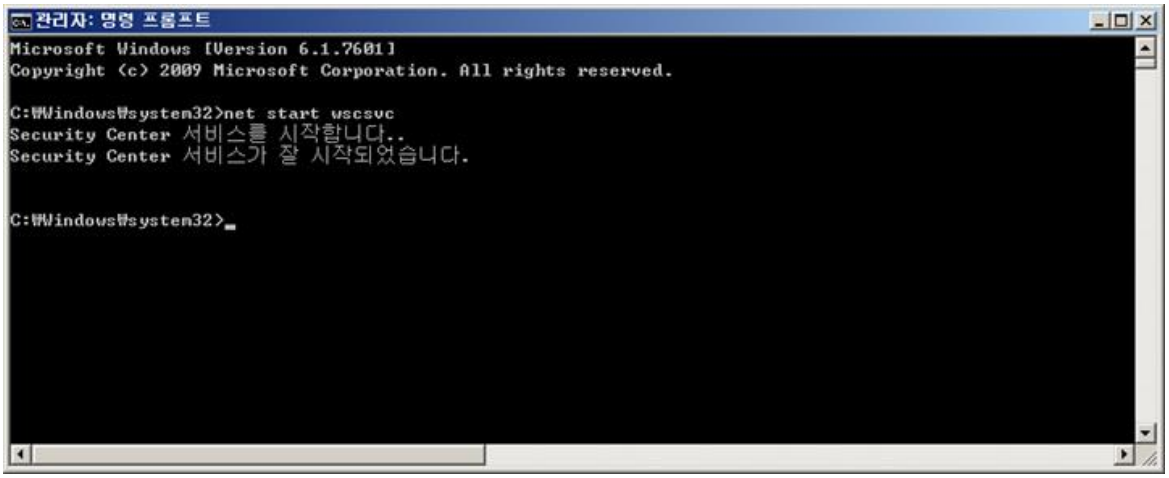


3. c:\windows\system32\wbem 폴더로 이동합니다. Repository 폴더의 이름을 다른 이름으로 변경 합니다.
   (예) Repository_abc

4. 명령어 창에 **net start winmgmt**를 입력합니다.



5. 명령어 창에 **net start wscsvc**를 입력합니다.



6. PC를 다시 시작합니다.
7. 바이러스 백신을 다시 설치 하고 보안 센터를 확인합니다.
8. 내PC지키미를 실행 후 점검 시작을 다시 실행하고 점검 결과를 확인합니다.

참고

보안정보 집합체를 재 설정한 이후에도 점검 결과가 취약인 경우에는 관리자에게 문의하시거나 시스템 운영 체제를 다시 설치해야 할 수도 있습니다.

Q2. 바이러스 백신이 최신업데이트 상태임에도 바이러스 백신의 최신 보안 패치 점검이 취약으로 표시됩니다.

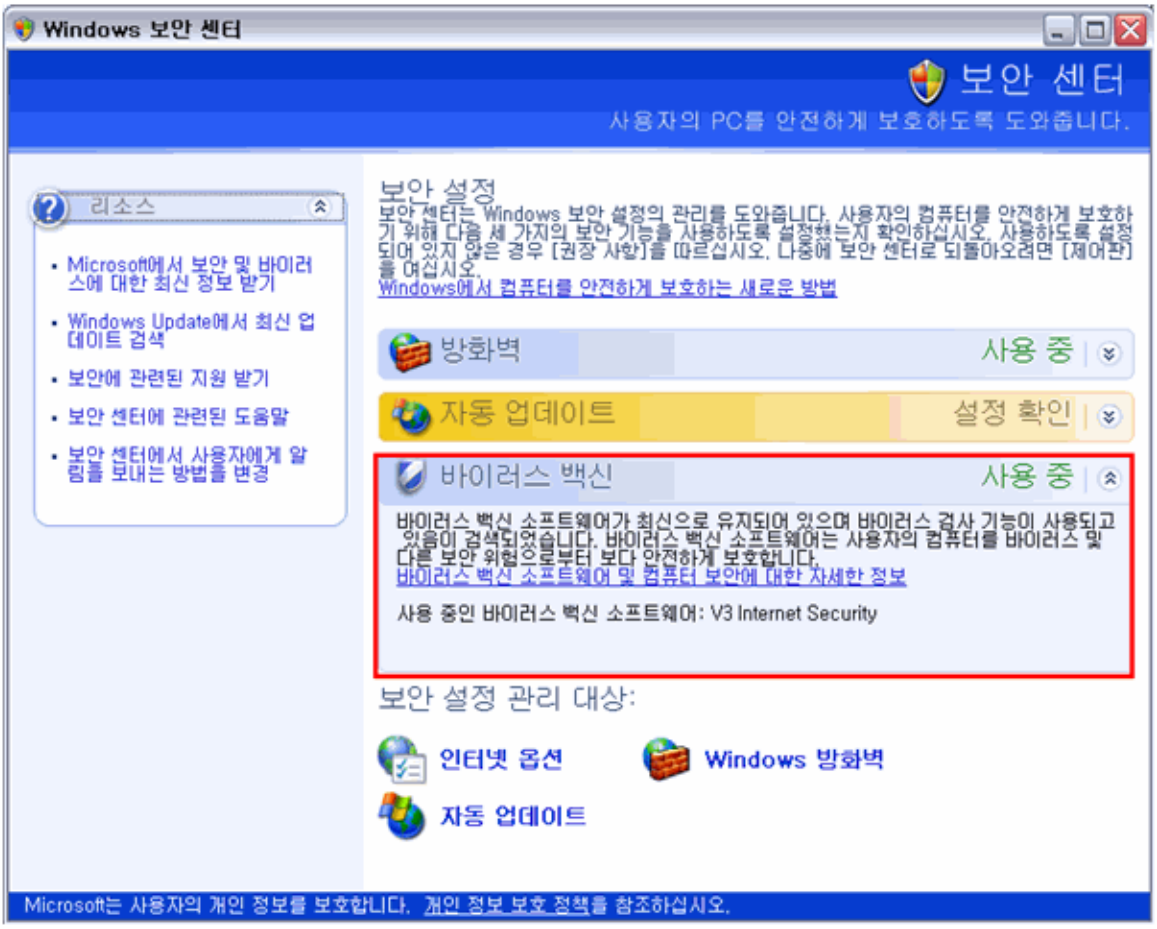
사용 중인 Windows 에 맞는 내 PC 지키미를 설치하십시오. Windows Vista 나 Windows 7 의 경우 내 PC 지키미 버전이 권장 버전 보다 낮은 경우 점검 결과가 다르게 표시될 수 있습니다.

참고

바이러스 백신 설치 및 실행 점검은 제어판의 보안 센터에 등록된 백신 정보를 기반으로 점검합니다.

보안 센터에서 바이러스 백신 정보 확인하기

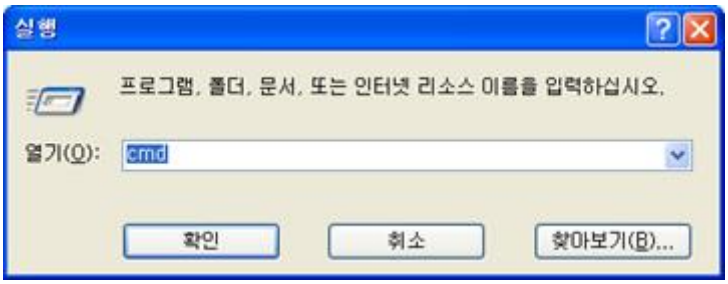
보안 센터는 Windows XP SP2 이상에서만 사용할 수 있으므로 사용 중인 PC 의 Windows 가 서비스 팩 2 이상인지 확인해 주십시오.



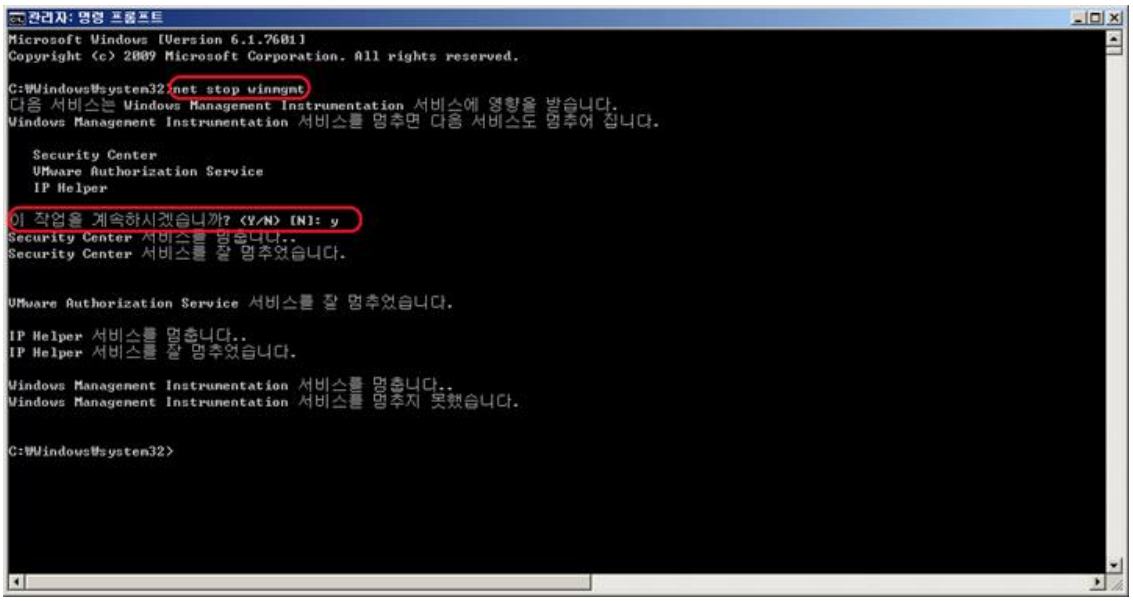
- 서비스 팩 2 이상인 경우 보안 센터에서 사용 중인 백신 제품의 정보가 표시되고 사용 중으로 표시되는지 확인하십시오.
- 바이러스백신 정보가 찾을 수 없음이나 사용 안 함으로 표시되면 점검 결과는 취약으로 표시됩니다.
- 백신이 설치되어 있는 경우에 보안 센터에 해당 정보가 표시되지 않는 이유: 설치된 백신 제품에서 Windows 보안 센터에 정보를 제공하지 않거나 설치 정보가 일치하지 않기 때문입니다.
- 보안 센터에서 바이러스 백신 정보가 사용 중으로 표시되지만 점검 결과가 취약인 경우: 시스템 보안 정보 집합체를 재설정하십시오.

시스템 보안정보 집합체 재설정 하는 방법

1. **시작** > **실행**을 누른 후 입력 창에 **cmd**를 입력합니다.

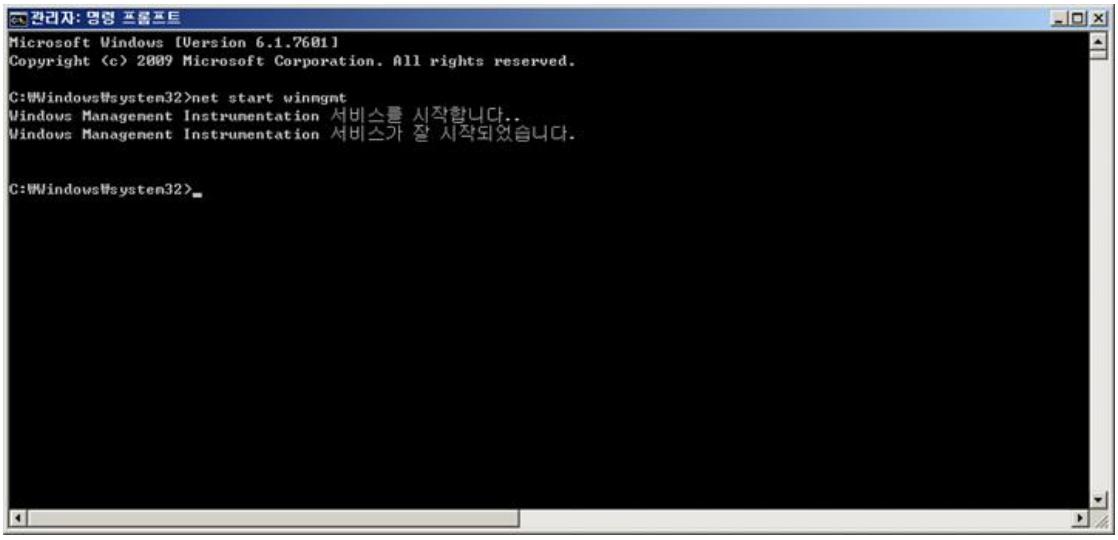


2. 명령어 창에 **net stop winmgmt**를 입력합니다. ***서비스를 멈추면 다음 서비스도 멈추어집니다. 이 작업을 계속 하시겠습니까?** 라는 메시지에 **Y**를 입력합니다.

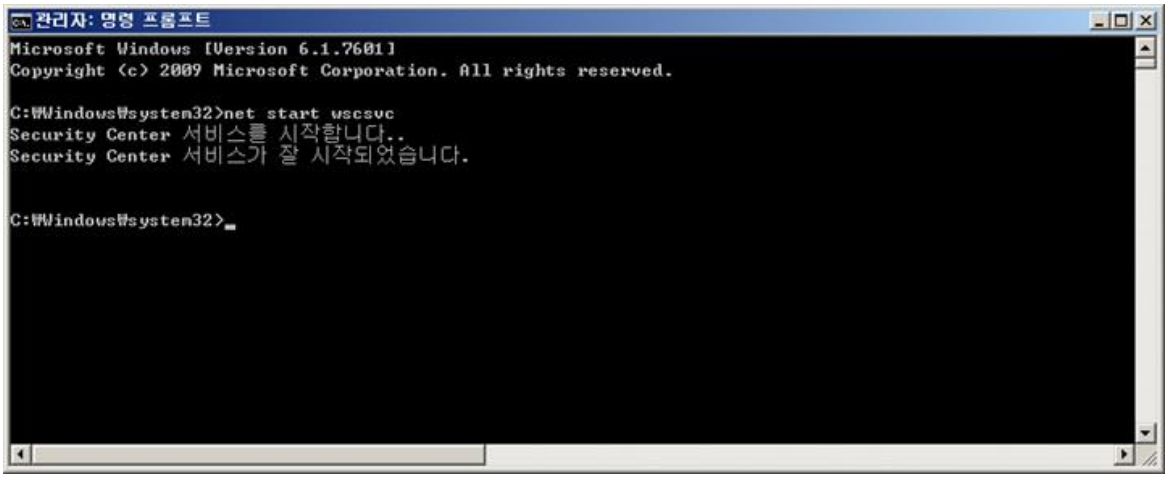


3. c:\windows\system32\wbem 폴더로 이동합니다. Repository 폴더의 이름을 다른 이름으로 변경 합니다. (예) Repository_abc

4. 명령어 창에 **net start winmgmt**를 입력합니다.



5. 명령어 창에 **net start wscsvc**를 입력합니다.



6. PC를 다시 시작합니다.
7. 바이러스 백신을 다시 설치 하고 보안 센터를 확인합니다.
8. 내PC지키미를 실행 후 점검 시작을 다시 실행하고 점검 결과를 확인합니다.

참고

보안정보 집합체 재설정 이후에도 점검 결과가 취약인 경우에는 담당자에게 문의하시거나 시스템의 운영 체제를 다시 설치해야 할 수도 있습니다.

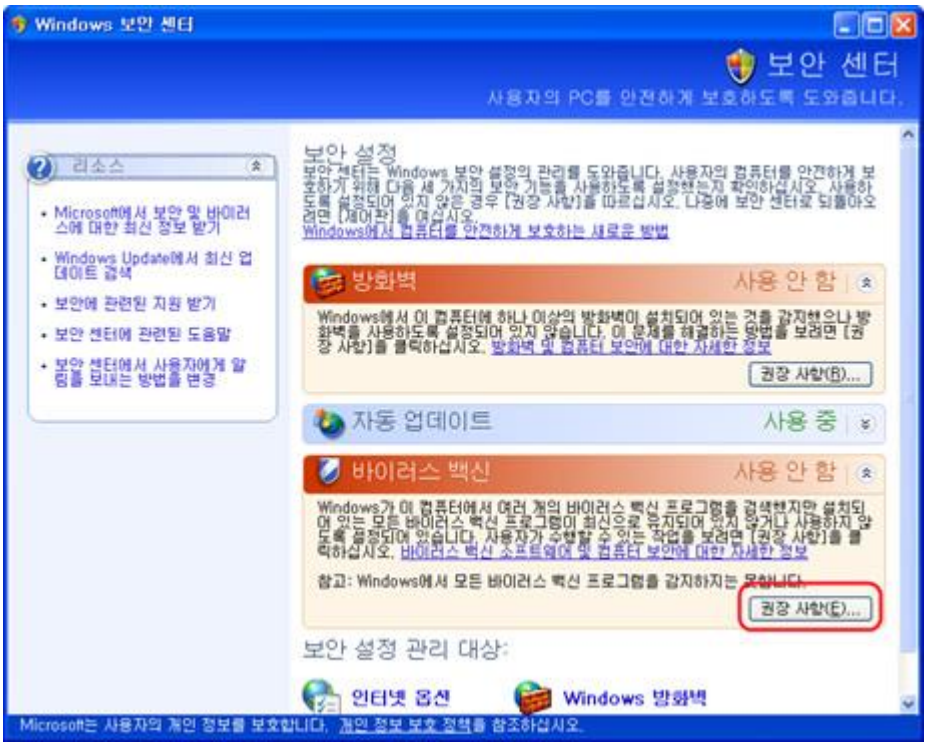
Q3. 바이러스 백신 관련 점검 결과가 점검 불가로 표시됩니다.

Windows 의 보안 센터에서 사용자가 직접 관리하는 바이러스 백신 프로그램을 사용하고 있습니다. 옵션을 선택한 경우에는 점검 결과가 점검 불가로 표시됩니다. 내 PC 지키미에서 바이러스 백신 점검을 하려면 보안 센터의 해당 옵션을 선택 해제해야 합니다.

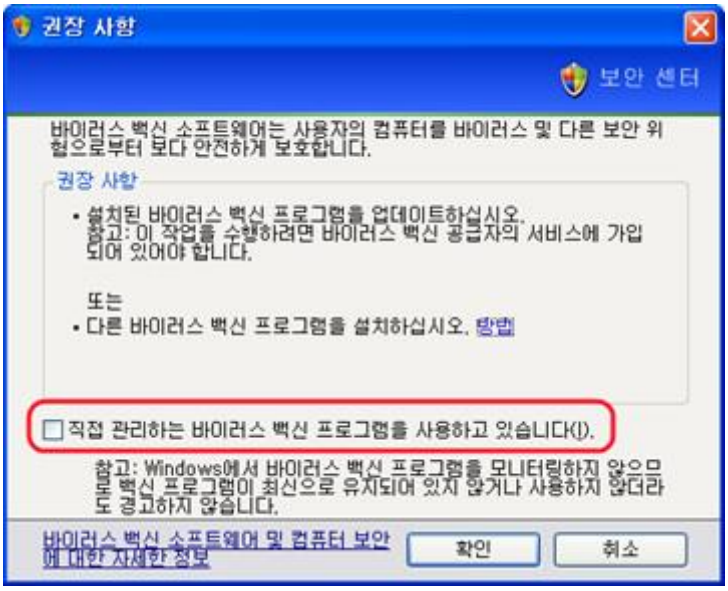
보안 센터 확인

보안 센터에서 옵션을 확인합니다. 제어판에서 보안 센터 화면을 확인할 수 없으면, 보안 센터 서비스 실행 여부를 확인합니다.

1. **시작** > **제어판**에서 **보안 센터**를 실행합니다.
2. 보안 센터에서 바이러스 백신 영역에서 **권장 사항**을 선택합니다.



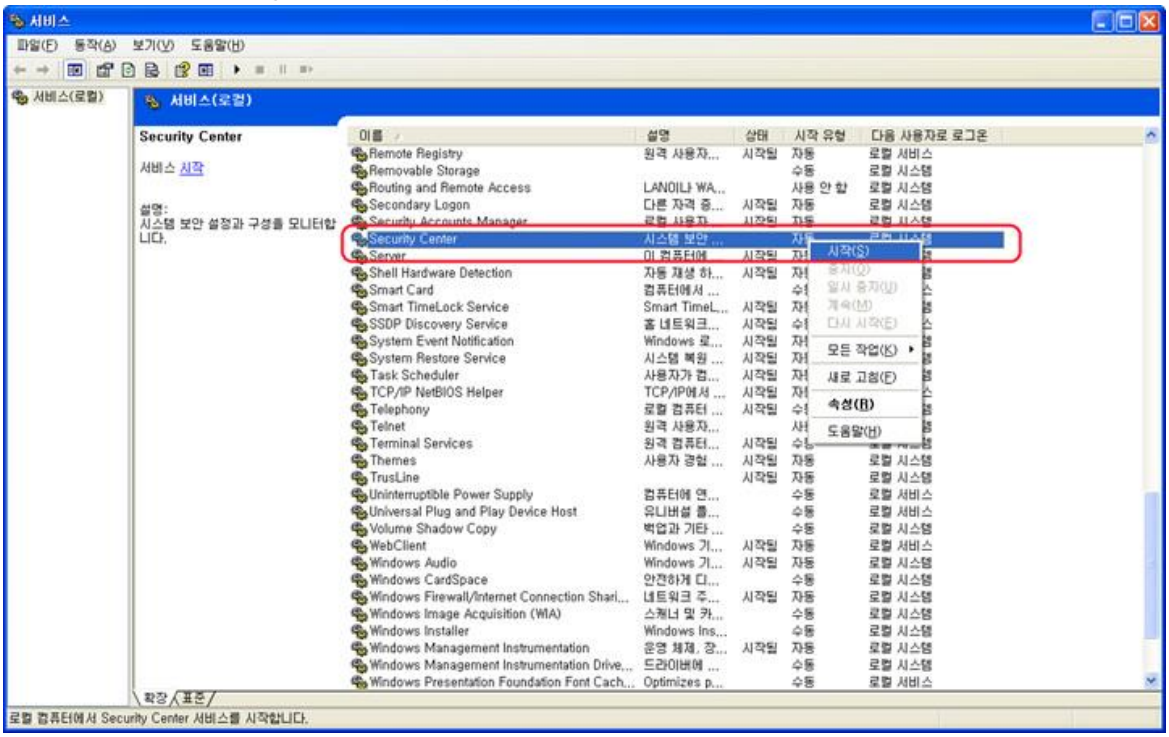
3. <권장 사항>에서 **직접 관리하는 바이러스 백신 프로그램을 사용하고 있습니다.** 를 선택 해제 합니다.



보안 센터 서비스 실행 여부

제어판에 **보안 센터**가 보이지 않는 경우에는 보안 센터 서비스를 직접 실행해 주십시오.

1. 윈도우 **시작** 메뉴를 클릭합니다.
2. 시작 > 제어판 > 관리도구 > **서비스**로 이동합니다.
3. <서비스>에서 **Security Center 서비스**(wscsvc)를 시작합니다.

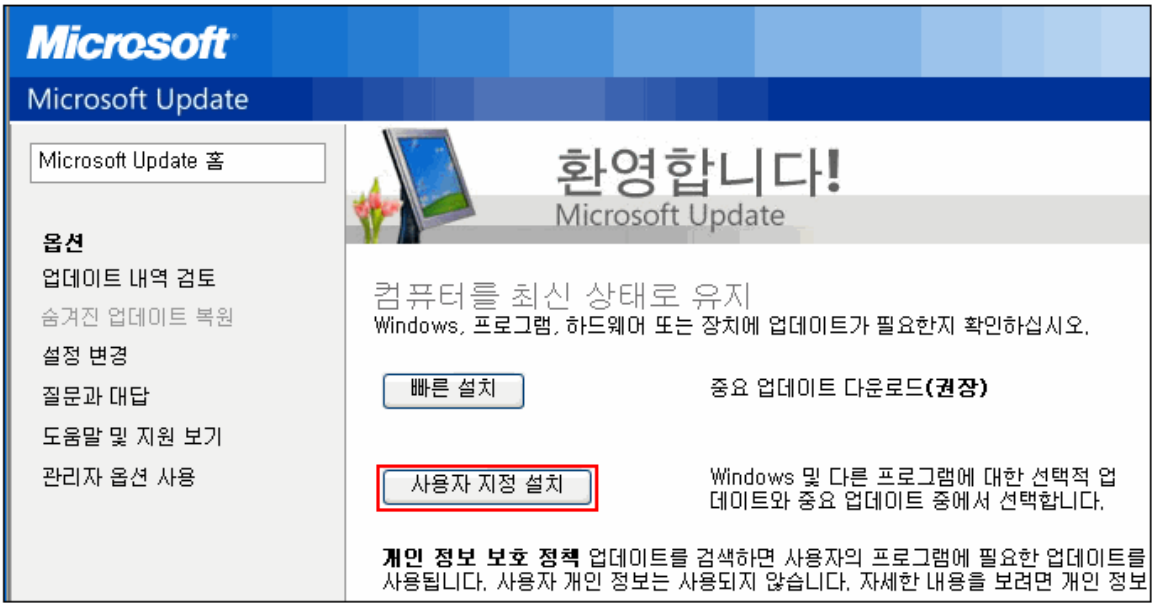


Q4. 설치하지 않아야 하는 MS 업데이트 항목을 꼭 설치해야 하나요?

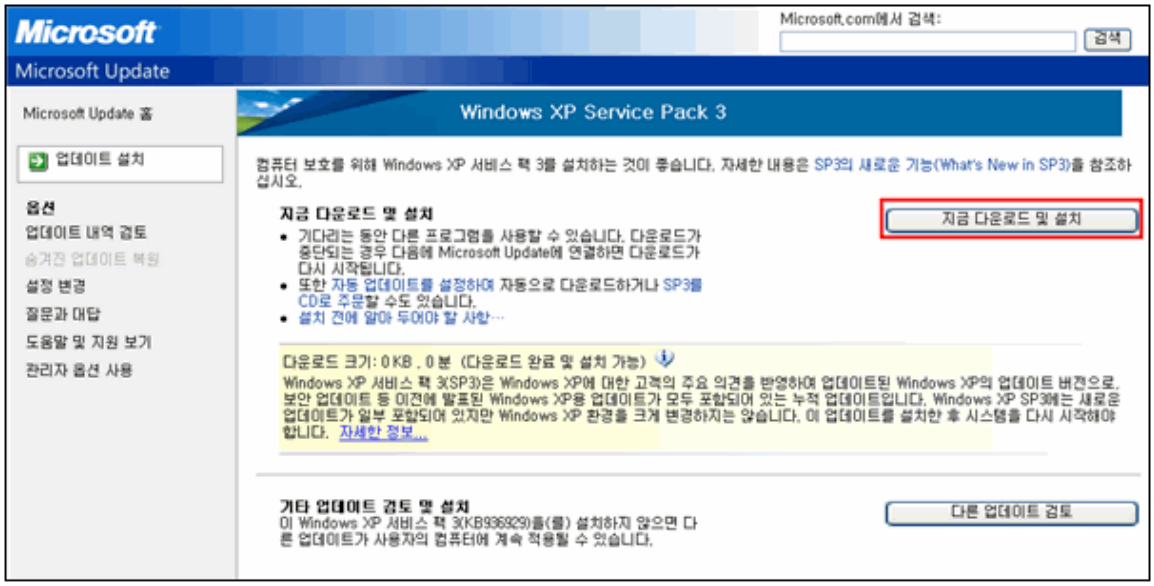
설치할 필요가 없는 업데이트는 업데이트 숨기기를 설정하면 점검 대상에서 제외됩니다. 업데이트 숨기기는 MS 정책에 따라 주기적으로 설정된 내용이 해제될 수 있으므로 설정이 해제된 경우에는 사용자가 직접 다시 설정해야 합니다.

업데이트 숨기기

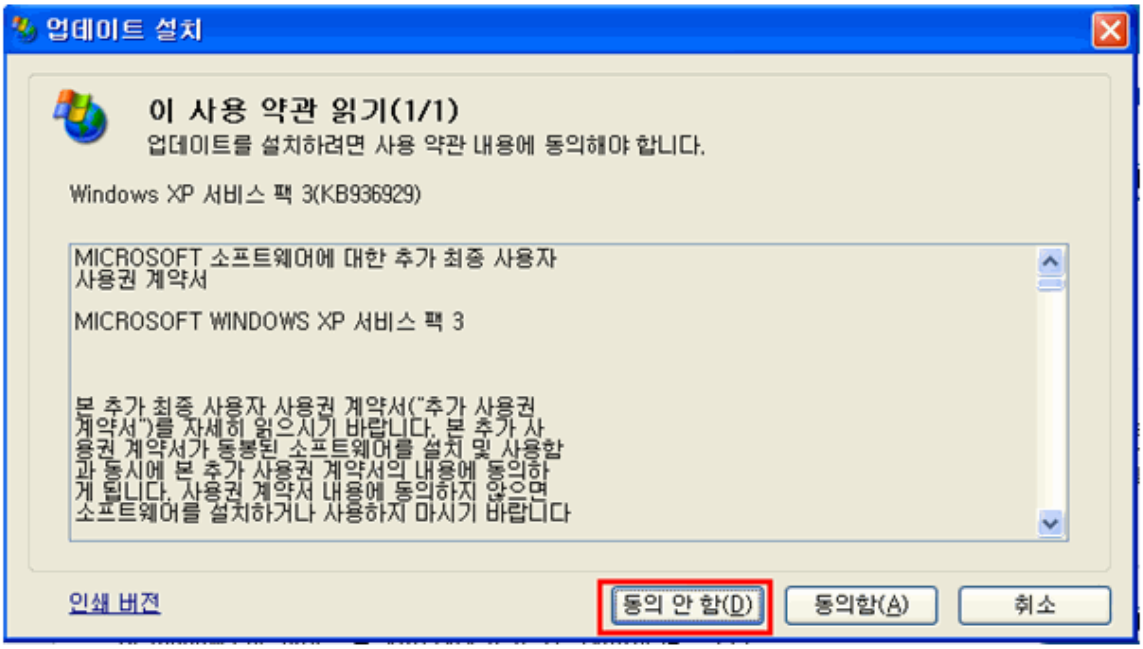
1. MS 업데이트 사이트(http://update.microsoft.com)에 접속합니다.
2. 업데이트 화면에서 **사용자 지정 설치**를 선택합니다.



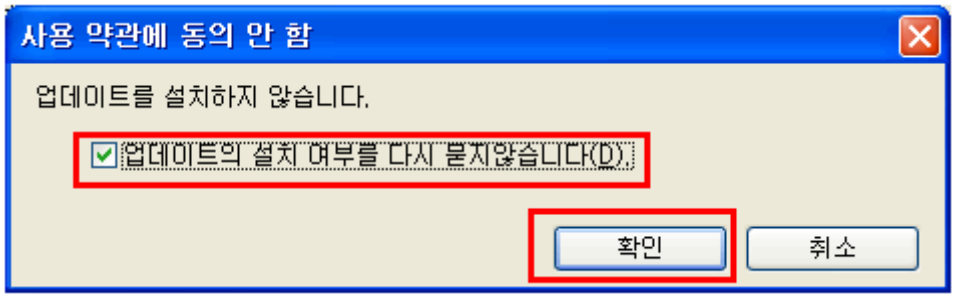
3. **지금 다운로드 및 설치**를 누릅니다.



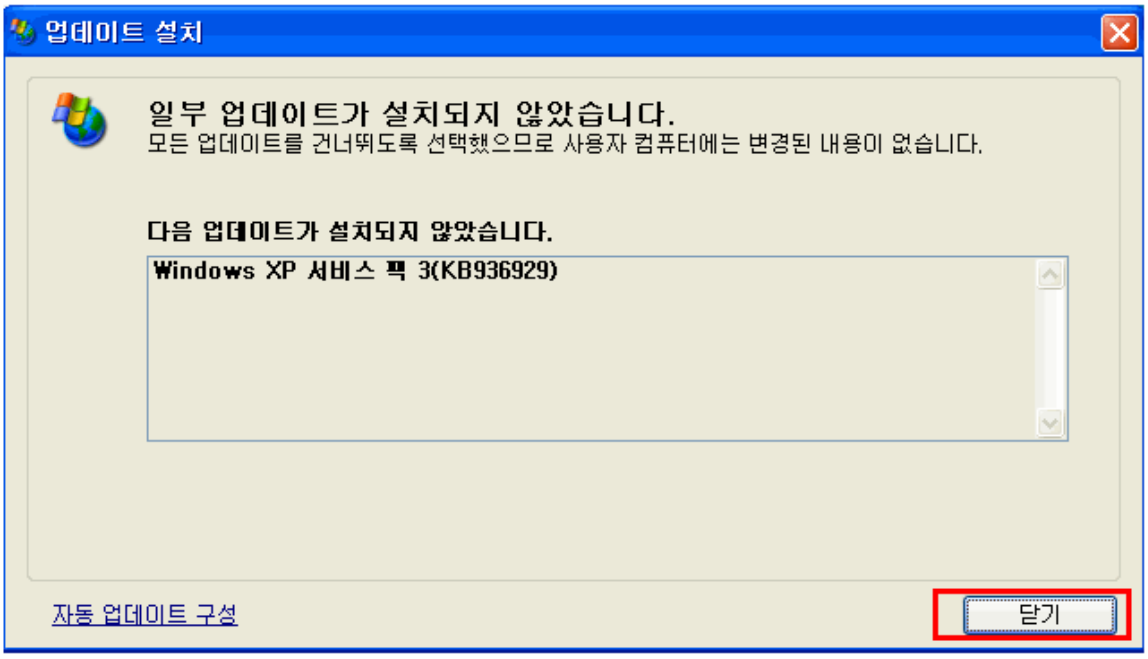
4. <업데이트 설치>가 나타나면 설치를 원하지 않는 항목에 대해 **동의 안 함**을 선택합니다.



5. <사용 약관에 동의 안 함>이 나타나면, **업데이트의 설치 여부를 다시 묻지 않습니다.** 를 선택하고 **확인**을 누릅니다.

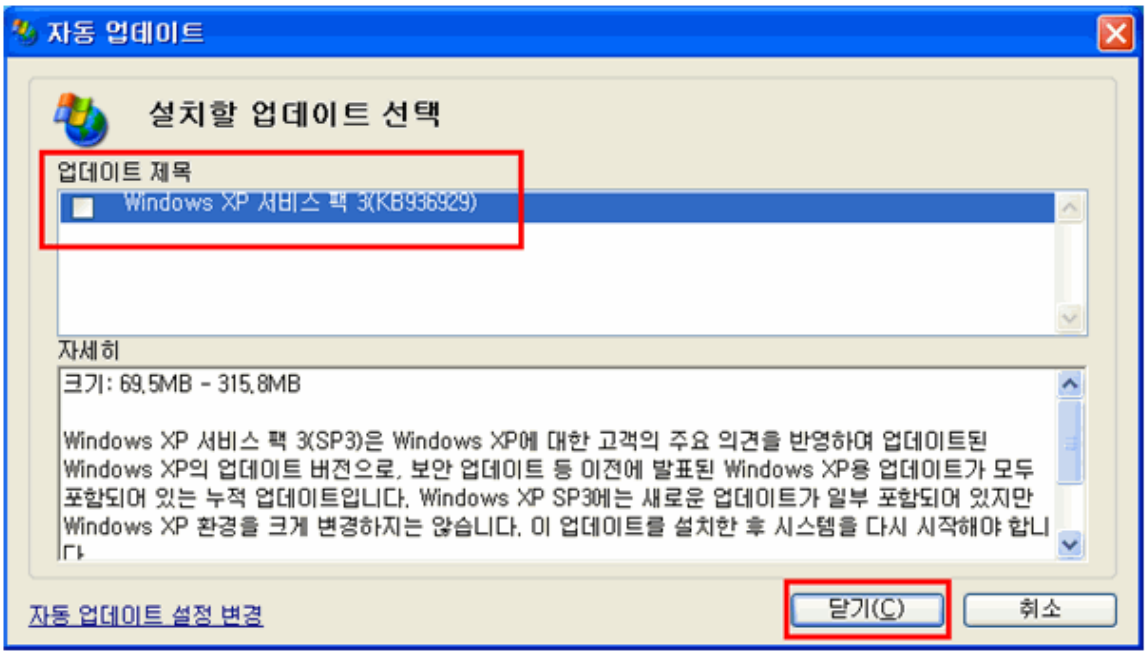


6. <업데이트 설치>에서 업데이트 완료 후 **일부 업데이트가 설치되지 않았습니다.** 라는 메시지가 표시되고 설치되지 않은 항목을 보여줍니다.



자동 업데이트( )에서 업데이트 숨기기

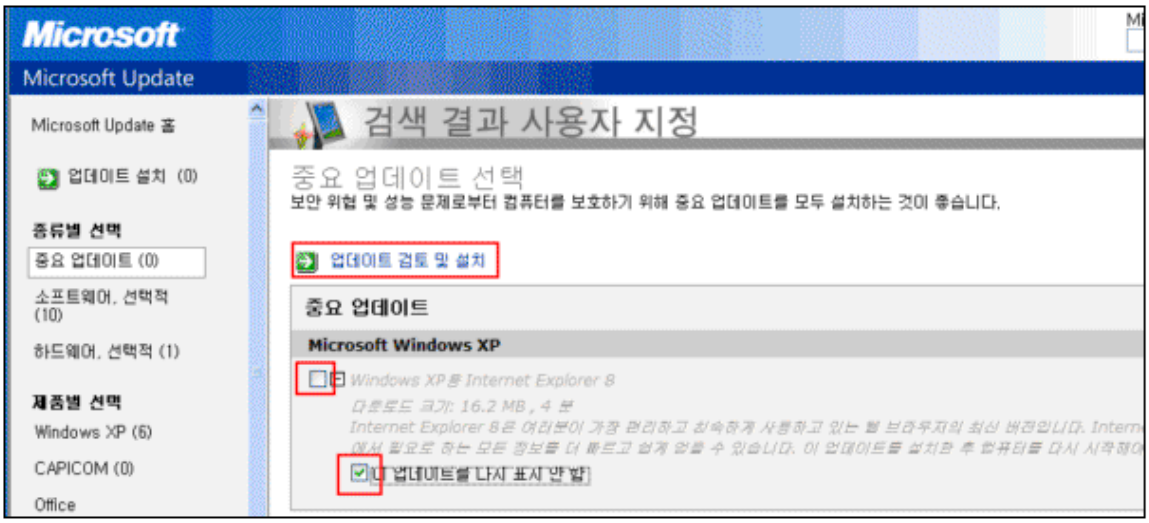
1. 작업 표시줄의 자동 업데이트 ( )을 선택합니다.
2. 사용자 정의 설치(고급)을 선택하고 **다음**을 누릅니다.
3. <자동 업데이트>의 업데이트 제목에 표시된 항목 중 설치하지 않을 항목을 선택 해제하고 **닫기**를 누릅니다.



4. <업데이트 숨기기>에서 **업데이트를 다시 알리지 않습니다.** 를 선택하고 **확인**을 누릅니다.

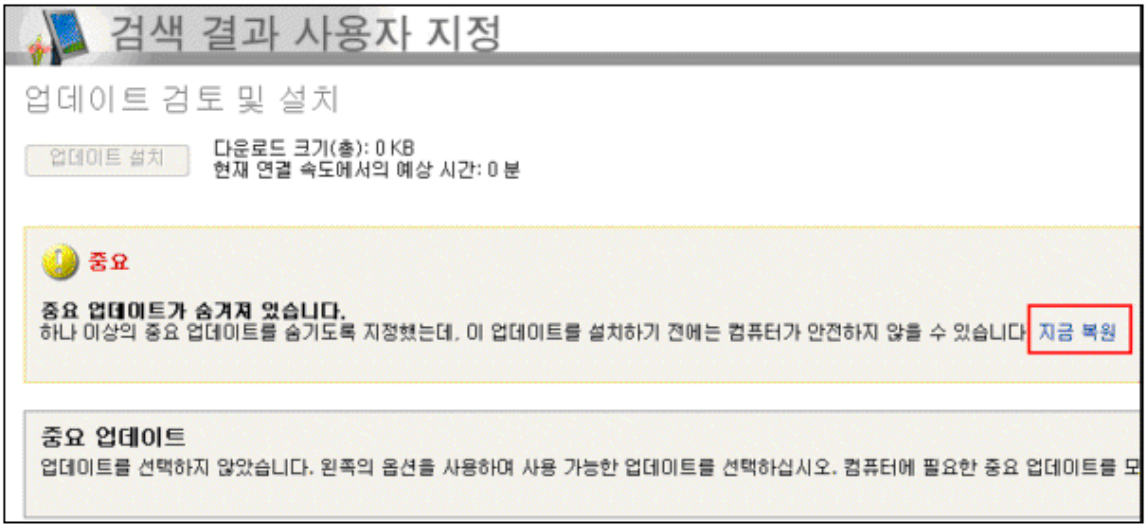
MS 홈페이지에서 업데이트 숨기기

1. MS 업데이트 사이트(http://update.microsoft.com)에 접속합니다.
2. 업데이트 목록에서 설치를 원하지 않는 항목의 선택을 해제하고, **이 업데이트를 다시 표시 안 함**을 선택합니다.



숨긴 업데이트 항목 표시

1. MS 업데이트 사이트(http://update.microsoft.com)에 접속합니다.
2. 업데이트 화면에서 업데이트 검토 및 설치를 누릅니다.
3. 중요 업데이트가 숨겨져 있습니다. 메시지 영역에서 **지금 복원**을 누릅니다.



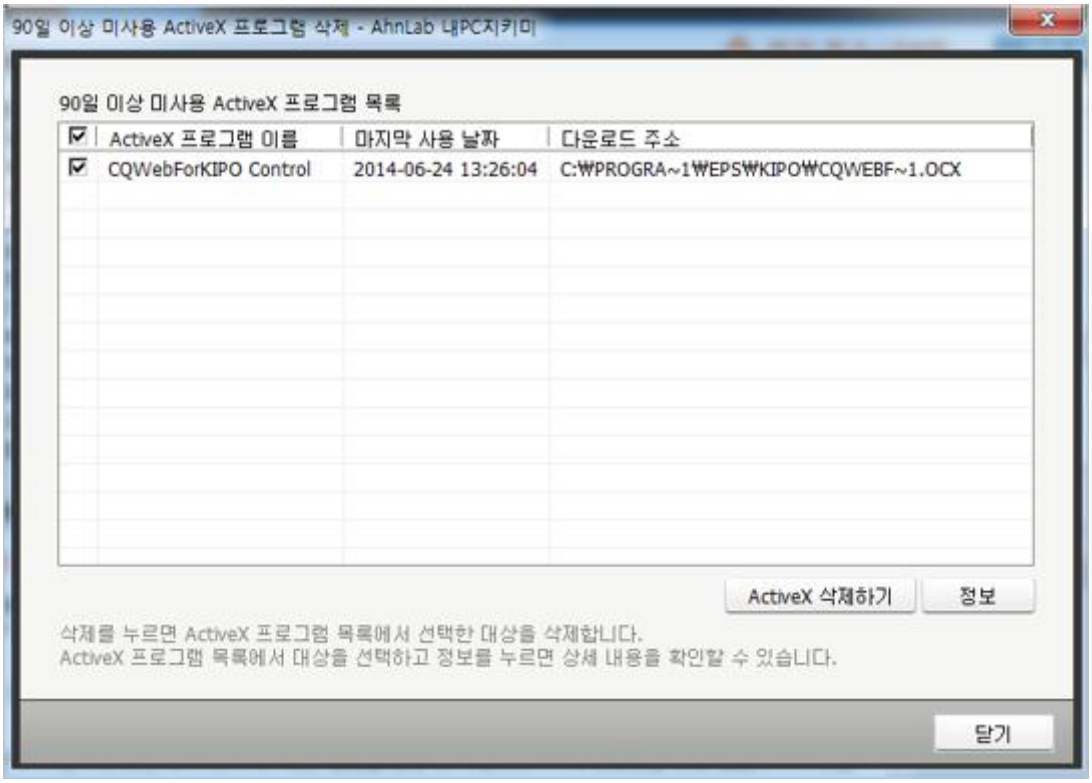
Q5. ActiveX 프로그램이 삭제되지 않습니다.

다른 프로세스가 ActiveX 프로그램을 사용하고 있는 경우 삭제되지 않을 수도 있습니다.

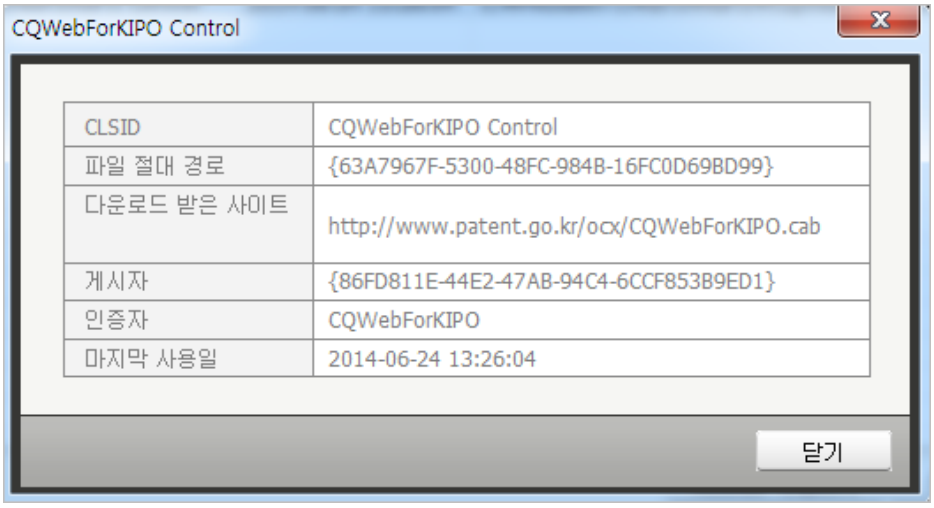
내 PC 지키미에서 ActiveX 삭제하기

ActiveX 삭제하기를 실행하면 설치된 ActiveX 목록 중 관리자가 설정한 기간 이상 사용하지 않은 ActiveX 목록을 확인할 수 있습니다. 사용자는 ActiveX 목록에서 필요 없는 항목을 직접 선택하여 삭제하거나 설치된 ActiveX 에 대한 상세 정보를 확인할 수 있습니다.

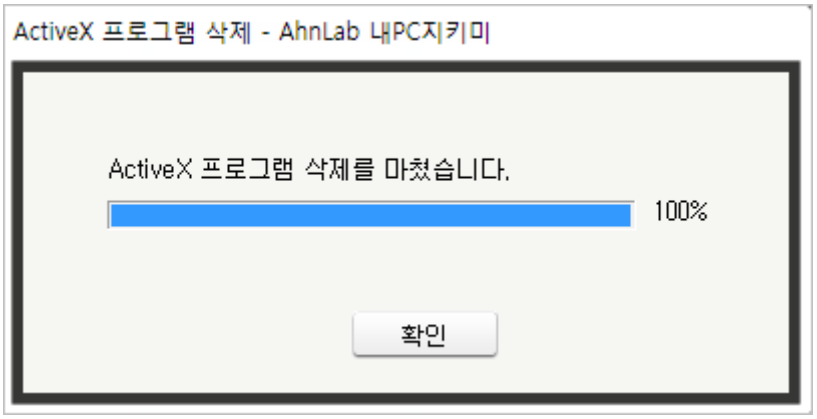
1. 미사용 ActiveX 프로그램 존재 점검 항목에서 취약으로 진단된 경우 점검 항목 상세 정보 옆에 있는 **ActiveX 삭제하기**를 실행합니다.
2. 미사용 ActiveX 프로그램 목록이 화면에 나타납니다. 목록에서 삭제할 대상을 선택한 후에 **ActiveX 삭제하기**를 누릅니다.



- ActiveX 프로그램 목록에 표시된 ActiveX 에 대한 상세 정보를 확인하고 싶으면 정보를 누릅니다.



3. 삭제 진행 과정이 표시되며, 삭제가 완료되면 **확인**을 눌러 창을 닫습니다.



참고

실행 중인 프로그램과 Internet Explorer 를 먼저 실행 종료하시기 바랍니다. 다른 프로세스가 ActiveX 프로그램을 사용하고 있는 경우 삭제되지 않을 수도 있습니다.

Q6. 내 PC 지키미 프로그램을 실행하였으나 오랫동안 화면이 나타나지 않습니다.

내 PC 지키미가 실행될 때 관리 서버인 PC 진단결과 확인시스템과 통신을 합니다. 개인 방화벽이 설치되어 있는 경우 내 PC 지키미가 서버로 보낸 요청 트래픽을 차단하여 실행 후 오랜 시간 화면이 나타나지 않을 수 있습니다.

방화벽 프로그램 확인

사용 중인 개인 방화벽 프로그램에서 내 PC 지키미 프로그램 관련 트래픽을 모두 허용으로 설정하십시오.

Q7. 내 PC 지키미 설치 후 바탕 화면에 바로 가기가 표시되지 않습니다.

내 PC 지키미를 다운로드 하여 설치한 후 계정 권한이 적절하지 않은 경우 바탕 화면의 아이콘이 생성되지 않을 수 있습니다.

1. 내 PC 지키미 정상 설치 여부 확인

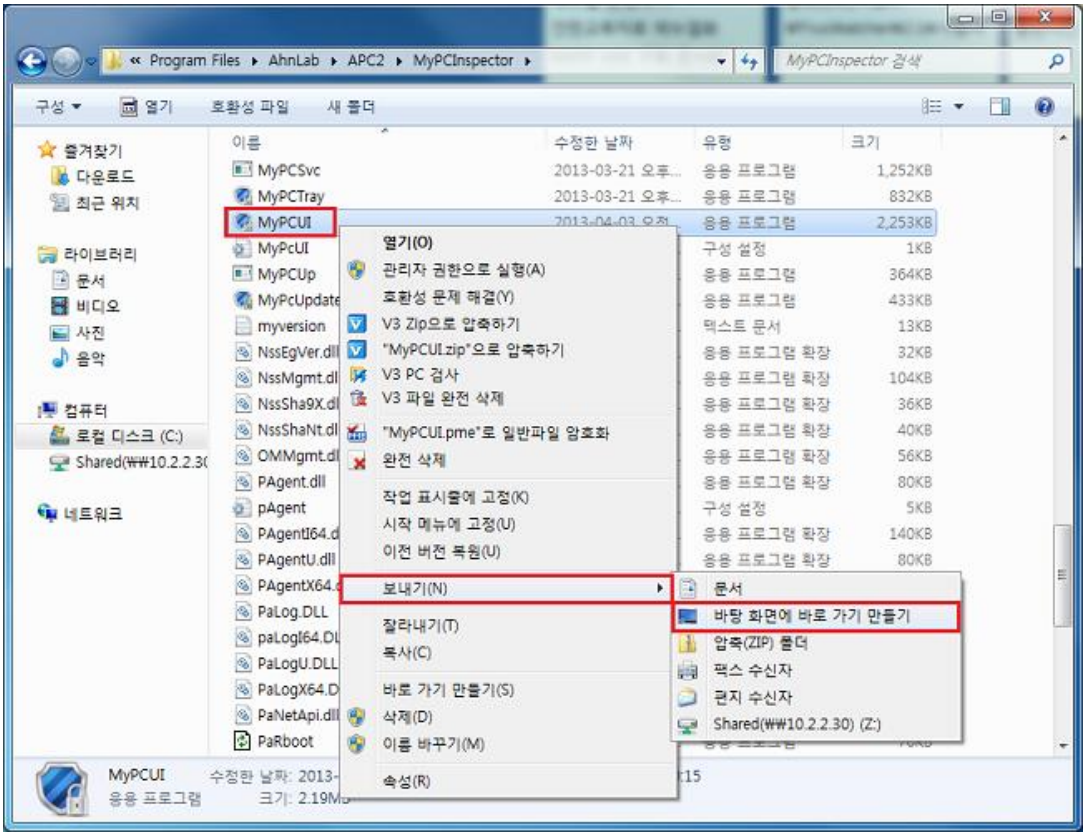
윈도우 탐색기에서 C:\Program Files\AhnLab\APC2\Policy Agent 폴더에 있는 MyPCUI.exe 를 직접 실행합니다. 아래 화면이 표시되는지 확인하고, 정상 실행되지 않을 경우에는 내 PC 지키미 프로그램이 정상 설치되지 않은 경우입니다.

참고

운영 체제가 64bit 시스템인 경우 C:\Program Files (x86)\AhnLab\APC2\Policy Agent 경로에 MyPCUI.exe 파일이 존재합니다.

2. 제품이 정상 설치된 경우 바탕 화면 아이콘 직접 만들기

1. 윈도우 탐색기를 실행합니다.
2. **C:\Program Files\AhnLab\APC2\MyPCInspector** 폴더에 있는 **MyPCUI.exe** 에서 마우스 오른쪽을 누른 후 **보내기** > **바탕 화면에 바로 가기 만들기**를 선택합니다.

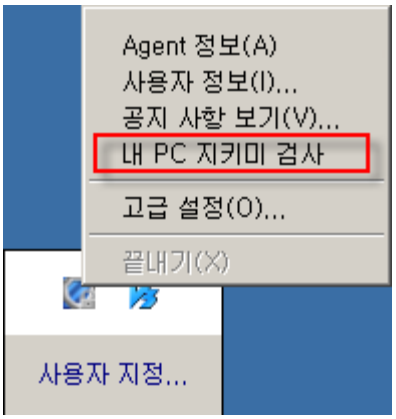

« Program Files ▸ AhnLab ▸ APC2 ▸ MyPCInspector ▸
MyPCInspector 검색
구성
열기
호환성 파일
새 폴더
즐겨찾기
다운로드
최근 위치
라이브러리
문서
비디오
사진
음악
컴퓨터
로컬 디스크 (C:)
네트워크
이름
수정한 날짜
유형
크기
MyPCSvc
MyPCTray
MyPCUI
MyPcUI
MyPCUp
myversion
PAgent.dll
pAgent
PAgentU.dll
PaLog.DLL
PaRboot
응용 프로그램
구성 설정
텍스트 문서
열기(O)
관리자 권한으로 실행(A)
호환성 문제 해결(Y)
V3 Zip으로 압축하기
"MyPCUI.zip"으로 압축하기
V3 PC 검사
V3 파일 완전 삭제
"MyPCUI.pme"로 일반파일 암호화
완전 삭제
작업 표시줄에 고정(K)
시작 메뉴에 고정(U)
이전 버전 복원(U)
보내기(N)
잘라내기(T)
복사(C)
바로 가기 만들기(S)
삭제(D)
이름 바꾸기(M)
속성(R)
문서
바탕 화면에 바로 가기 만들기
압축(ZIP) 폴더
팩스 수신자
편지 수신자
Shared(₩₩10.2.2.30) (Z:)
MyPCUI
응용 프로그램

Q8. 점검 항목이 보이지 않습니다.

내 PC 지키미 최초 설치 후 점검 항목이 확인되지 않는 증상은 정상이며, 에이전트 프로그램과 서버와의 통신 후에 점검 항목이 적용됩니다. 일반적으로 점검 항목의 적용에 많은 시간이 소요되지는 않으나 PC 점검일 등 서버의 부하가 많은 시점에는 다소 시간이 소요될 수 있습니다.

내 PC 지키미 검사 메뉴 확인

점검 항목이 적용되지 않은 상태에서는 작업 표시줄의 에이전트 아이콘( )의 마우스 오른쪽을 눌렀을 때, **내 PC 지키미 검사** 메뉴가 보이지 않습니다. 이런 경우는 PC 를 재 부팅 한 후, 점검 항목을 다시 확인합니다.



HOME 화면에서 점검 항목 확인

HOME 화면에서 **점검 시작**을 눌러 PC 점검을 수행합니다. 점검이 완료된 이후에도 점검 항목이 보이지 않는다면 점검에 필요한 파일들을 서버로부터 받지 못했을 경우일 수 있습니다. 이런 경우, 네트워크가 정상적인 상태인지 확인합니다.

Q9. 내 PC 지키미 검사는 어떻게 실행시키나요?

내 PC 지키미 검사를 수동으로 실행시키는 방법은 다음과 같습니다.

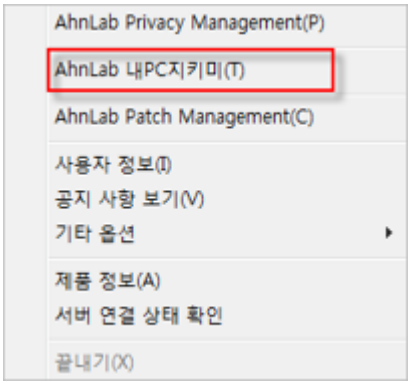
내 PC 지키미 메인 창을 통해 검사를 실행하는 방법

1. 바탕 화면의 AhnLab 내 PC 지키미 아이콘을 눌러 메인 창을 실행시킵니다.
2. 메인 창에서 **점검 시작** 버튼을 누릅니다.

트레이의 알림 아이콘을 통해 검사를 실행하는 방법

1. 바탕 화면의 작업 표시줄에 있는 에이전트 아이콘을 선택하여 오른쪽 마우스를 누릅니다.

2. **AhnLab 내PC지키미** 메뉴를 누릅니다.



3. **AhnLab 내PC지키미** 메뉴를 누르면 메인 창이 나타납니다. 실행된 메인 창에서 내PC지키미 검사를 수행할 수 있습니다.

Q10. 점검 점수가 0 점으로 나타납니다.

내 PC 지키미 점검을 수행하지 않은 경우, 점검 점수가 0 점으로 나올 수 있습니다.

PC 점검 미 실행

내 PC 지키미 점검을 수행하지 않아 미점검 점수인 0 점으로 표시 될 수 있습니다. 점검을 수행하지 않은 경우라면, PC 점검을 수행하십시오. 내 PC 지키미 메인 창을 통해 검사를 실행하는 방법은 다음과 같습니다.

1. 바탕 화면의 AhnLab 내 PC 지키미 아이콘을 눌러 메인 창을 실행시킵니다.
2. 메인 창에서 **점검 시작** 버튼을 누릅니다.

트레이의 알림 아이콘을 통해 검사를 실행하는 방법

1. 바탕 화면의 작업 표시줄에 있는 에이전트 아이콘을 선택하여 오른쪽 마우스를 누릅니다.

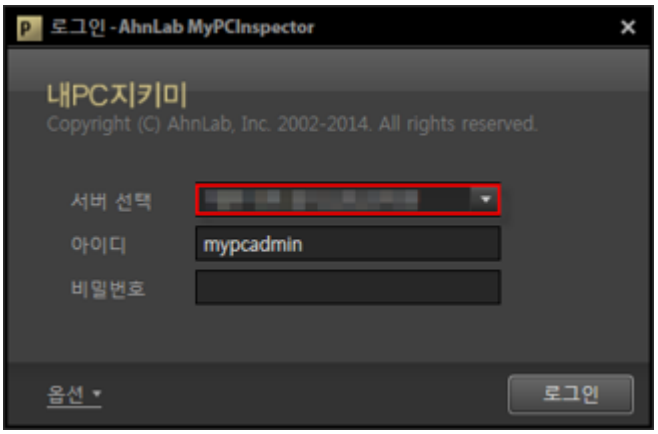
2. **AhnLab 내PC지키미** 메뉴를 누릅니다.

3. **AhnLab 내PC지키미** 메뉴를 누르면 1번의 메인 창이 나타납니다. 실행된 메인 창에서 PC 점검을 수행할 수 있습니다.

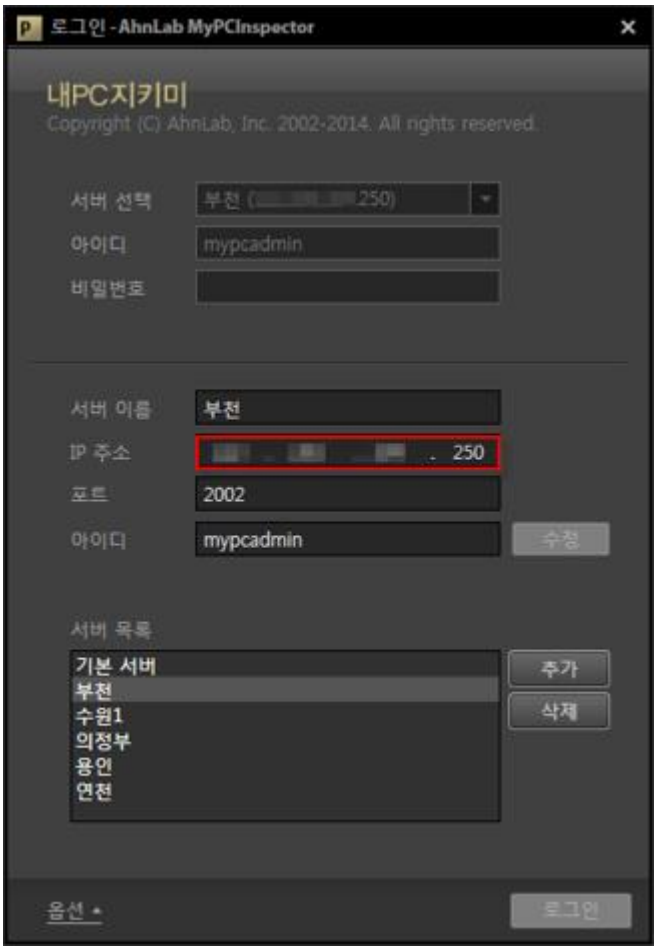
Q11. 관리 콘솔(MyPC Admin)을 설치한 후 서버에 접속이 되지 않습니다.

관리 콘솔 프로그램을 통하여 서버에 접속할 수 없습니다.

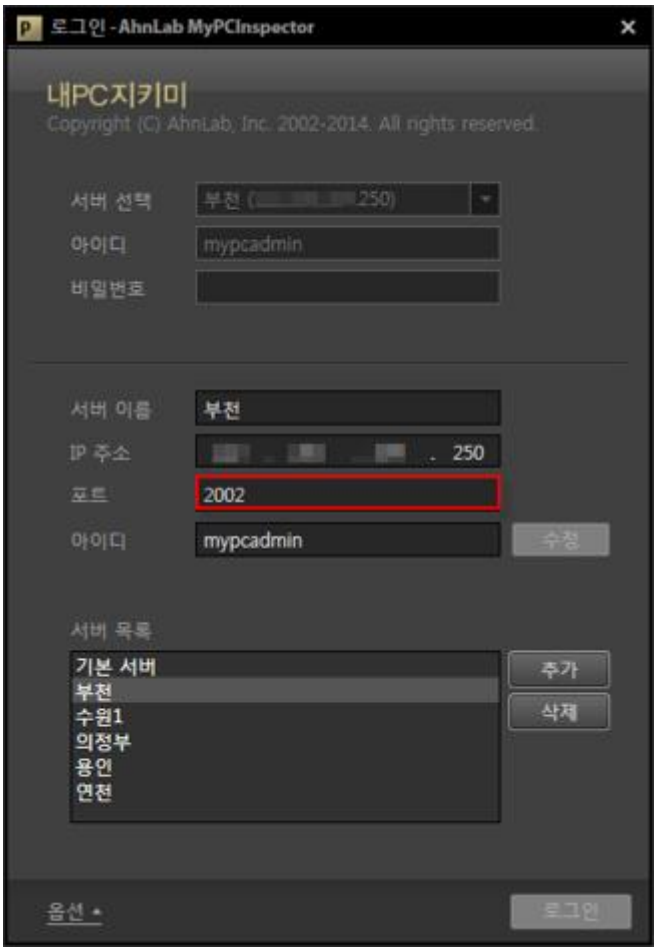
1. 서버의 입력 정보를 확인합니다. 서버 선택에 입력되어 있는 IP 정보가 정확한 정보인지 확인합니다.



2. 서버의 IP 가 잘못 입력되어 있는 경우 좌측 하단의 **옵션**을 클릭하여 IP 주소를 수정 후 재 로그 인을 시도합니다.



3. MyPC Admin 의 접속에 사용되는 포트 번호는 2002 입니다. 2002 외 다른 번호가 기입되어 있는 경우 로그인이 되지 않으니 2002 로 수정 후 재 로그 인을 시도 합니다.



4. 접속에 필요한 계정이나 서버 IP 를 모르는 경우, 관리자에게 문의하십시오.

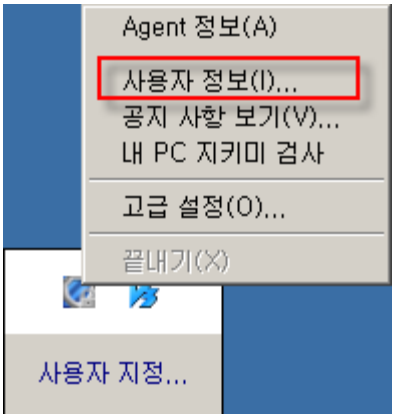
Q12. 사용자 정보는 어떻게 편집하나요?

PC 를 사용하는 사용자가 변경이 되는 경우 사용자 정보 편집이 필요합니다.

사용자 PC 에서 알림 아이콘을 통한 사용자 정보 편집

작업 표시줄에 있는 Policy Agent 의 아이콘( )을 누르면, 사용자 정보를 에이전트 사용자가 직접 입력할 수 있습니다.

1. 작업 표시줄의 에이전트 아이콘( )에서 마우스 오른쪽을 눌러 **사용자 정보**를 선택합니다.
2. <사용자 정보>가 나타나면 항목을 입력합니다.

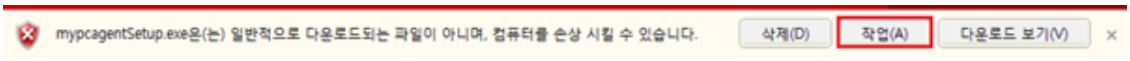


3. <사용자 정보>가 나타나면 변경된 사용자 이름을 입력한 후, 확인 버튼을 누릅니다.

Q13. 내 PC 지키미의 에이전트 설치 파일이 다운로드 되지 않습니다.

사용중인 Windows 환경에 따라 SmartScreen 필터 기능으로 인하여 정상적으로 다운로드 되지 않는 경우가 발생할 수 있습니다. 이는 사용자의 Windows 환경에 따른 사항으로, 정상적인 서버 IP 로 접속하여 파일을 다운로드 받는 경우 다음과 같이 조치하십시오.

1. 다음과 같은 화면이 나타나면 **작업** 버튼을 선택합니다.



2. 다음 화면에서 좌측 하단의 **기타 옵션**을 선택합니다.

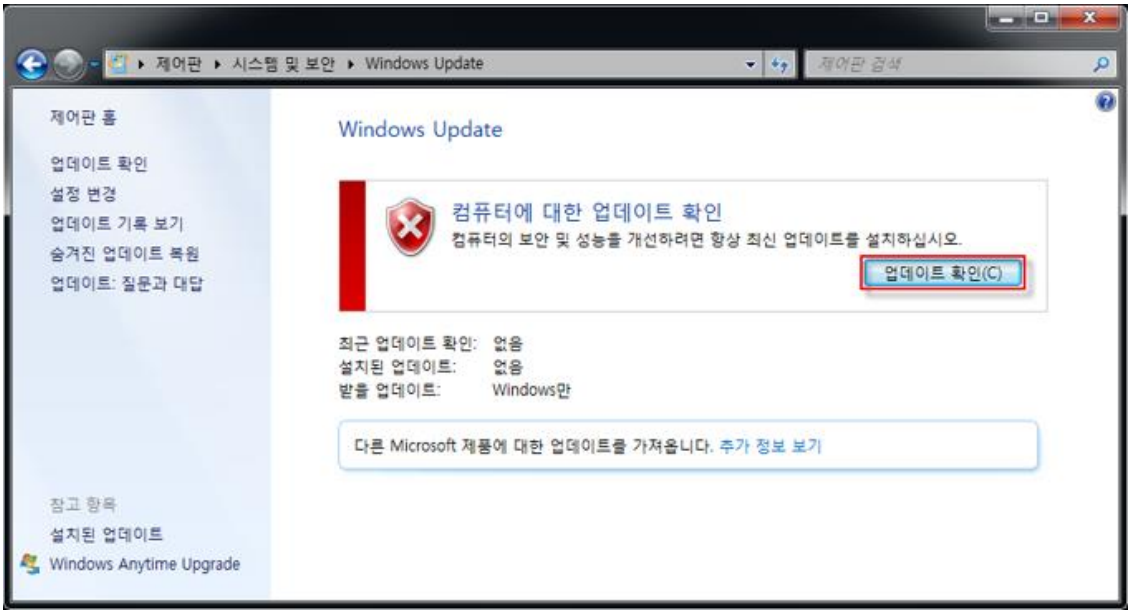
3. 다음 화면에서 **실행** 버튼을 누르면 에이전트의 설치 과정이 진행됩니다. 에이전트가 설치되지 않은 PC 의 경우 설치가 진행되고, 에이전트가 설치되어 있으면 기존 에이전트를 삭제한 후, 재 설치가 진행됩니다.

Q14. 운영체제, MS Office 최신 보안 패치 여부 점검이 취약으로 보입니다.

운영 체제, MS Office 최신 보안 패치에 대한 업데이트를 진행합니다.

1. 시작 메뉴의 **Windows Update** 기능을 이용하여 최신 보안 패치를 적용 합니다.

2. 최신 보안패치가 적용되어 있지 않은 경우 다음과 같은 화면이 보이며 **업데이트 확인** 버튼을 눌러 업데이트를 실행합니다.



3. 업데이트 완료 후 적용을 위해서는 반드시 PC를 재 부팅 하여야 하며 재 부팅 후 남아있는 보안패치가 추가로 있지는 않은지 다시 확인을 진행한 후 재 점검을 실행합니다.

색인

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: http://www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901