AhnLab 내 PC 지키미

에이전트 사용설명서

Ahnlab

목차

일러 두기	5
고객시원 연락저	6
I 상 실시 아기	
시스템 사양	
에이선트 설시하기	9
2 장 시작 하기	10
보안 점검	
보안 점검의 날	
패스워드 안전성 검사	
3 장 HOME	17
경제 설명	
4상 PC 점검	20
PC 점검	
기본 취약점 점검 목록	
보안 업네이트	
패스워드 안선성 검사	
와면 모오기 열정····································	
ㅇㅠ ᆯ딕 ᆯᆼ ㅂ아 ㅍㄹㄱ래 선치	
과리자 추가 점검	
확장 취약점 점검 목록	
Windows 설정 점검	41
계정 설정 점검	45
로컬 보안 정책	53
네트워크 설정 점검	56
웹 브라우저 설정 점검	68
기타 점검	76
5 장 패스워드 점검 도구	89
패스워드 점검	
6 장 PC 최적화	91
PC 최적화	
7장 보고서	94
으 · · · · · · · · · · · · · · · · · · ·	
8 장 점검 결과와 조치 방법	
기본 취약적 적건 목록	99
바이러스 백신 설치 및 실행 점검	
바이러스 백신의 최신 보안 패치 점검	

	운영 체제, MS Office 최신 보안 패치 점검	.110
	한글 프로그램의 최신 보안 패치 점검	.126
	로그온 패스워드 안전성 점검	.129
	로그온 패스워드 사용 기간 점검	.136
	화면 보호기 설정 점검	.137
	사용자 공유 폴더 설정 점검	.140
	미사용 ActiveX 프로그램 점검	.141
	USB 자동 실행 설정 점검	.143
	비인가 프로그램 설치 점검	.144
	보안 USB 설치 점검	.146
	무선 랜카드 설치 점검	.147
	편집 프로그램 설치 점검	.148
	PDF 프로그램의 최신 보안 패치 점검	.149
확징	· 취약점 점검 목록	152
	Windows 이벤트 로그 덮어쓰기 설정 점검	152
	사용자 계정 컨트롤(UAC) 설정 점검	.155
	보안 센터 서비스 실행 점검	.157
	Windows 자동 업데이트 설정 점검	161
	Administrators 그룹 내 사용자 계정 점검	.163
	패스워드 암호화 알고리즘 설정 점검	166
	장기간 미접속 계정 점검	.167
	패스워드 사용 기간 제한 설정 점검	170
	Guest 계정 사용 점검	.173
	사용 안 함 계정 점검	.175
	Administrator 계정 사용 점검	.181
	Windows 자동 로그온 점검	.183
	패스워드 최대/최소 사용 기간 설정 점검	.189
	최근 사용한 패스워드 사용 점검	.191
	Windows 로그온 실패 횟수 초과 시 계정 잠금 설정 점검	.192
	인터넷 연결 공유 사용 점검	.196
	원격 사용자의 시스템 공유 디렉터리 접속 가능 점검	. 199
	무선 랜카드 사용 점검	.203
	비인가 사용자 접근 제어(NULL Session 접근 제어) 점검	204
	FTP 서비스 실행 점검	206
	웹 서비스 실행 점검	208
	Simple TCP/IP 서비스 실행 점검	210
	Windows 방화벽 사용 점검	.212
	원격 데스크톱 포트 변경 점검	.214
	원격 데스크톱 사용 점검	.219
	IE ActiveX 컨트롤 및 플러그 인 실행 점검	.221
	IE 종료할 때 검색 기록 삭제 점검	.224
	IE 파일 다운로드 사용 점검	.226
	IE 사용자 이름/암호 자동 완성 설정 점검	.229

	IE ActiveX 컨트롤 다운로드 설정 점검	232
	IE 신뢰할 수 있는 사이트 목록의 취약성 점검	235
	IE 사용자 인증 시 자동 로그온 설정 점검	238
	IE 종료 시 임시 인터넷 파일 삭제 점검	241
	Adobe Flash Player 최신 업데이트 점검	243
	데이터 실행 방지(DEP) 사용 점검	245
	개인 정보 미처리 파일 개수 초과 점검	247
	소프트웨어 저작권 점검 프로그램 실행 점검	250
	사용자 정의 취약점 점검	252
	전체 공유(Everyone) 권한의 공유 폴더 사용 점검	253
	하드디스크 파일 시스템의 NTFS 사용 점검	255
	NTP 시간 서버와 자동 동기화 설정 점검	257
	Adobe AIR 최신 업데이트 점검	
	Java SE Runtime Environment 최신 업데이트 점검	
	hosts 파일 내 비허용 IP 점검	
	비허용 DNS 설정 점검	
	문서 보호 기능 점검	
9 잔	위제	
- 0	의제 기는	271
10 T	· · ·································	
10 2	방 작업 표시굴	
	사용사 성보	273
	공지사항 보기	274
	고급 설정	
	세품 성보	276
11 장	당 자주하는 질문(FAQ)	277
	Q1. 바이러스 백신이 설치/실행되고 있는데도 바이러스 백신 설치 및 실행 점검이 '취약'으로	
	표시됩니다	278
	Q2. 바이러스 백신이 최신업데이트 상태임에도 바이러스 백신의 최신 보안 패치 점검이 취약!	으로
	표시됩니다	
	Q3. 바이러스 백신 관련 점검 결과가 점검 불가로 표시됩니다	
	Q4. 설치하지 않아야 하는 MS 업데이트 항목을 꼭 설치해야 하나요?	
	Q5. ActiveX 프로그램이 삭제되지 않습니다	
	Q6. 내 PC 지키미 프로그램을 실행하였으나 오랫동안 화면이 나타나지 않습니다	292
	Q7. 내 PC 지키미 설치 후 바탕 화면에 바로 가기가 표시되지 않습니다	293
	Q8. 점검 항목이 보이지 않습니다	295
	Q9. 내 PC 지키미 검사는 어떻게 실행시키나요?	
	Q10. 점검 점수가 0 점으로 나타납니다	298
	Q11. 관리 콘솔(MyPC Admin)을 설치한 후 서버에 접속이 되지 않습니다	
	Q12. 사용자 정보는 어떻게 편집하나요?	
	Q13. 내 PC 지키미의 에이전트 설치 파일이 다운로드 되지 않습니다	
	Q14. 운영체제, MS Office 최신 보안 패치 여부 점검이 취약으로 보입니다	
색인	<u>l</u>	306

일러 두기

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

© 2017 AhnLab, Inc. All rights reserved. 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 비밀번호를 입력하고 로그온을 누릅니다.)
PC 점검 > 점검 시작	'>'이 포함된 굵은 글꼴은 메뉴 실행 경로를 나타냅니다.
🚯 참고	제품을 사용할 때 참고할 사항입니다.
Å 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
- 운영시간: 평일오전 9시~오후 6시(토, 공휴일제외)
- 제품 정보: <u>http://www.ahnlab.com</u>의 제품 구매 > 구매처 안내

기업고객 기술지원

- 전화 번호: 1577-9431
- 운영시간: 평일오전 9시~오후 8시(토, 공휴일제외)
- 팩스: 031-722-8901

1장

설치 하기

시스템 사양 에이전트 설치하기

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
		Microsoft Windows XP Professional(SP2 이상)
		Microsoft Windows XP Home(SP2 이상)
		Microsoft Windows XP Media Center(SP2 이상)
	32 비트	Microsoft Windows Server 2003 R2 Standard(SP1 이상)
		Microsoft Windows Server 2003 R2 Enterprise(SP1 이산)
		Microsoft Windows Server 2002 P2 Datacenter(SP1 014)
		$M_{1} = 0$ $M_{1} = 0$ 2002 P2 $M_{1} = 0$ (SP1 0 4)
		Microsoft Windows Server 2003 R2 Web(SP1 이상)
		Microsoft Windows XP Professional x64
	64 비트	Microsoft Windows Server 2003 R2 Standard x64
	•	Microsoft Windows Server 2003 R2 Enterprise x64
		Microsoft Windows Server 2003 R2 Datacenter x64
		Microsoft Windows Vista Home Basic K/KN
		Microsoft Windows Vista Home Premium K
		Microsoft Windows Vista Business K
	32/64 비트	Microsoft Windows Vista Enterprise
운영 체제		Microsoft Windows Vista Ultimate K
시스템 종류		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
	52/04 01=	Microsoft Windows Server 2008 R2 Datacenter
	모두 지원	Microsoft Windows Server 2008 K2 web Server
		Microsoft Windows 7 Professional
		Microsoft Windows 7 Elltimate
		Microsoft Windows 8
		Microsoft Windows 8
		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.

← → Ø http://	/AgentInstall/lis	st_agent.htm 🛛 🔎 👻 🖒	<i>i</i> AhnLab EMS 🛛 🗙	☆ ☆ छ	3
파일(F) 편집(E) 보기(V)	즐겨찿기(A) 도구(T)	도움말(H)			
					~
		에이저트 서귀 피아			
	,	에이신드 열지 파달			
다운로드 파일	설명		파일변경 날짜		
🔯 mypcagentSetup,exe	LHPC	지키미 설치 파일	2015-07-23 17:32:10		
	Copyright(c) Ahn	Lab, Inc. 2002-2014. All right			
				<u></u>	_
				• 100% -	н

- 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(之)이 표시됩니다.

한참고

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 시작을 누릅니다.

AhnLab Lipo	지키미					
HOME	PC 점겸	패스위드 점검 도구	PC 최적화	보고서		
			최근 점경	걸과 2016), 06, 01, 10:18 (결과 전송 완료)	
				_	49건	
		A	히막	9 건		
		근 PC 점검 점수	83 87	- 22		
		85점	점겸 점수	추이	최근 1회	
			· (85점)			
			06/01			
			DC 최정창	un	PC 최적화 실행	
	- <u>PC 점경 점수</u> (<u>반영 항목</u>	Fourt	27	다음 점검일까지 남은 날짜: 14일	

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.

정검 완료 - AhnLab 내PC지	₹ □		×
본 PC에 대한 취약	혐 점검을 다음과 같이	비 완료했습니다.	
안전	안전한 항목	49 건	
취약 점검 불가	취약점 발견 항목 점검 불가 항목	9건 2건	
점검 결과 진송	황 완료(2016-06-0	1 10:25)	
			*101

5. **확인**을 누르면 창이 닫힙니다.

한참고

안전, 취약, 점검 불가 항목에 대한 상세 내용은 <u>PC 점검</u>에서 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.

보안 점검의 날 - AhnLab 내PC지키미	23
보안 점검의 날입니다. 유하다.ab 내PC지키미에서 PC 점검을 수행하고 취약 항목을 조치하며 PC의 보안 수준을 강화하시기 바랍니다.	
안전 41건 취약 14건 점검 불가 0건	
다음 보안 사항에 대해 다시 한 번 진단해 주시기 바랍니다. 1. 운영 체제, MS Office의 최신 보안 패치 적용 2. 바미러스 백신의 최신 업데미트 적용 3. 의심스러운 미메일은 열람하지 말고 즉시 삭제 4. 로그온 패스워드에 대한 안전성 점검 및 주기적인 패스워드 변경 5. 전체 공유(Everyone) 권한의 공유 폴더 사용 금지	

한참고

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.

점검 완료 - AhnLab 내PC지키	0		
본 PC에 대한 취약점	점검을 다음과 같이	완료했습니다.	
<u>안전</u> 취약	안전한 항목 취약점 발견 항목	49 건 9 건	
점검 불가 감	점겸 불가 항목 완료(2016-06-01	2 건 10:25)	_
			확인

3. 점검 결과에 대한 상세 내용을 확인하려면 내PC지키미의 PC 점검 탭에서 점검 결과를 확인하여 필요 한 조치를 취합니다.

🛃 AhnLab 내PC지키미				
HOME PC 점검	레스워드 점검 도구 PC 최적화	보고서		
점겸 내용		🛕 점:	법 점수 : 85점 👘 점경	김 시작
전체 점검 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 하면 보호기 설정 - 공유 홀더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로럴 보안 정책 점검	항목 * 바이러스 백신 설치 및 실행 점검 바이러스 백신의 최신 보안 패치 점검 운영 체제, MS Office 최신 보안 패치 점검 한글 프로그램의 최신 보안 패치 점검 로그온 패스워드 안전성 점검 로그온 패스워드 안전성 점검 호면 보호기 설정 점검 사용자 공유 풀더 설정 점검 USB 자동 실행 설정 점검	2	결과 ▼ 안전 안전 안전 안전 안전 안전 안전 안전	
제건 차용 산내 정법	▼ 미사용 ActiveX 프로그램 점검		취약	Ŧ
점검 양쪽 상세 정도 점검 결과: 안전 PC에 바이러스 백신이 설치되어	1 있고, 백신미 실행 중입니다.		수 <u>조치 방법 상</u>	AL CATH

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.

패스워드 안전성 검사 - AhnLab 내PC지키미	23
패스워드 안전성 검사를 위해 Windows의 패스워드를 입력하십시오.	
Windows 로그온 패스워드를 입력하십시오.	-
확인 후	휘소

4. 보안 점검 진행 화면이 나타납니다.

보안 김	점검 중 - AhnLab 내PC지키미	
Γ	보안 점검은 1~10분 정도 소요되며 보안 점검 중에는 다른 작업을 실행하지 마십 시오, 운영 체제나 프로그램을 업데이트 하지 않은 PC는 점검 시간이 더 오래 걸 릴 수 있습니다.	
L	문서 보호 기능 점검 처리 중입니다. 점검 진행률 98%	

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

점검 완료 - AhnLab 내PC지	7 0		×
본 PC에 대한 취약점	성 점검을 다음과 같이	비 완료했습니다.	
안전 취약 점경 불가	안전한 향목 취약점 발견 항목 점겸 불가 항목	49 건 9 건 2 건	
정감 결과 전송) 완료(2016-06-0	1 10:25)	
			확인

- 6. **확인**을 누르면 창이 닫힙니다.
- 7. 내PC지키미의 PC 점검 탭에서 취약점 점검 결과를 확인합니다.

HOME PC 점검	페스위드 점검 도구	PC 최적화	보고서		
점겸 내용			🔒 🔒	령검 점수 : 85점	점검 시작
전체 정경 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 - 로럴 보안 정책 점검 - 네트워크 설정 점검	▲ 한목 ▼ 바이러스 백신 설치 바이러스 백신의 최신 운영 체제, MS Office 한글 프로그램의 최신 로그온 패스워드 안전 로그온 패스워드 안전 로그온 패스워드 사용 화면 보호기 설정 점 사용자 공유 폴더 설 USB 자동 실행 설정	및 실행 점검 신 보안 패치 점검 e 최신 보안 패치 점검 신 보안 패치 점검 전성 점검 용 기간 점검 검 점 점검 점검 점검	김	결과 * 안전 안전 안전 안전 안전 안전 안전 안전	
점겸 항목 상세 정보 점겸 결과: 안전 PC에 바이러스 백신이 설치5	티어 있고, 백신이 실행 중입니	Cł.		수 - - - - - - - - - - - - - - - - - - -	법상사안내

한참고

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

3장

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 날짜로 구성되어 있습니다.

AhnLab LijP	C지키미					
HOME	PC 점겸	패스위드 점검 도구	PC 최적화	보고서		
			최근 점검	결과 2016,	06, 01, 10:18 (결과 전송 완료)	
					49건	
		4	취막 전격 불기	9건 9건		
	ŧ	[근 PC 점검 점수	저거지스	*0I	オフリガ	
		85점		÷0	381 - 138	
			85점			
			06/01 10:18			
			PC 최적화	날짜		
	▶ <u>PC 점겸 점수</u>	<u>반영 항목</u>			다음 점검일까지 남은 날짜: 14일	

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.

4장

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 내용과 각 점검 항목에 대한 점검 항목 상세 정보로 구성되어 있습니다.

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

🔽 AhnLab LIPCX[7][]						
HOME PC 점검 피스	느위드 점검 도구	PC 최적화	보고서			
점검 내용			🔒 🦀 2	절검 점수 <mark>: 85</mark> 점	점검 시작	
전체 점검 목록 ▲ 기본 취약점 점검 목록 ▲ 보안 업데이트 - 패스워드 안전성 검사 - - 하면 보호기 설정 - - 모유 폴더 설정 - - 보안 프로그램 설치 - - 관리자 추가 점검 * 확장 취약점 점검 - - 계정 설정 점검 - - 로칠 보안 정책 점검 - - 네티의금 선정 적검 -	한목 ▼ 바이러스 백신 설 바이러스 백신의 운영 체제, MS Of 한글 프로그램의 로그온 패스워드 로그온 패스워드 화면 보호기 설정 사용자 공유 플더 USB 자동 실행 설	치 및 실행 점경 최신 보안 패치 점경 fice 최신 보안 패치 점경 안전성 점경 사용 기간 점경 점경 설정 점경 정 점경	점 점 검	겉과 ▼ 안전 안전 안전 안전 안전 안전 안전 안전		
점검 항목 상세 정보		프그램 영업		위목		
점겸 결과: 안전 PC에 바이러스 백신이 설치되어 있	!고, 백신이 실행 중입	JLICH.		^ <u>조치</u> ま	방법 상세 안내	

점검 내용

점검 내용은 기본 취약점 점검 목록과 확장 취약점 점검 목록으로 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 PC에 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. <u>보안 점검</u>을 실행하여 점검 결과를 확인합니다.
- 2. 점검 완료 창을 닫은 후 내PC지키미의 PC 점검 탭을 선택합니다.
- 점검 내용의 기본 취약점 점검 목록 > 보안 업데이트에서 바이러스 백신 설치 및 실행 점검을 선택합니다.

AhnLab ЦРС⊼ 考 □					
HOME PC 점검	피스워드 점검 도구	PC 최적화	보고서		
점겸 내용			🔺 i	점검 점수 <mark>: 85</mark> 점	점검 시작
전체 점겸 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 초면 보호기 설정 - 포유 폴더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - 제정 설정 점검 - 로컬 보안 정책 점검 - 네트워크 설정 점검	▲ 한목 ▼ 바이러스 백신 설 바이러스 백신의 운영 체제, MS O 한글 프로그램의	치 및 실행 점검 최신 보안 패치 점검 ffice 최신 보안 패치 최신 보안 패치 점검	5 점검 5		· · · · · · · · · · · · · · · · · · ·
점겸 항목 상세 정보					
점검 결과: 안전 PC에 바이러스 백신이 설치	되어 있고, 백신이 실행 중압	알니다.			1 바비 사내 아내
				*	

- 4. 바이러스 백신 설치 및 실행 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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

• <u>바이러스 백신 설치 및 실행 점검</u>

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. <u>보안 점검</u>을 실행하여 점검 결과를 확인합니다.
- 2. 점검 완료 창을 닫은 후 내PC지키미의 PC 점검 탭을 선택합니다.
- 점검 내용의 기본 취약점 점검 목록 > 보안 업데이트에서 바이러스 백신의 최신 보안 패치 점검을 선택 합니다.

🛃 AhnLab 내PC지키미					- • ×
HOME PC 점검	패스워드 점검 도구	PC 최적화	보고서		
점겸 내용			A :	점검 점수 <mark>: 85</mark> 점	점감 시작
전체 점검 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 초면 보호기 설정 - 공유 폴더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 로럴 보안 정책 점검 - 네트워크 설정 점검	▲ 향목 ▼ 바이러스 백신 설 바이러스 백신의 운영 체제, MS O 한글 프로그램의	치 및 실행 점검 최신 보안 패치 점검 ffice 최신 보안 패치 최신 보안 패치 점검	1 점검 1		과 · · · · · · · · · · · · · · · · · · ·
점겸 항목 상세 정보					
점검 결과: 안전 PC의 바이러스 백신이 최신:	으로 업데이트되어 있습니다	Ъ.		<u>م</u>	<u>치 방법 상세 안내</u>

- 바이러스 백신의 최신 보안 패치 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: 바이러스 백신 프로그램에 최신 보안 패치가 적용되어 있는 경우입니다.
 - 취약: 바이러스 백신 프로그램에 최신 보안 패치가 적용되지 않은 경우입니다. 관리 센터 실행하기를 눌러 보안 센터에 등록된 바이러스 백신이 최신 업데이트 상태인지 확인합니다. 바이러스 백신이 최신 업데이트 상태가 아닌 경우, 지금 업데이트를 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. <u>보안 점검</u>을 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.

🔀 AhnLab ЦРС⊼(₹ □		
HOME PC 점검	페스워드 점검 도구 PC 최적화 보고서	
점겸 내용	🚹 점검 점수	: 85점 점검 시작
전체 점검 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 호면 보호기 설정 - 공유 폴디 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 로럴 보안 정책 점검 - 너트워크 설정 점검		겉과 ▼ 안전 안전 안전 안전
점겸 항목 상세 정보		*
담김 글과: 안전 PC의 운영 체제 및 MS Offic * Microsoft에서 지정한 중/ 다	e가 최신 상태입니다. 3 업데이트가 모두 설치되어 있는 경우에만 점검 결과가 '안전'으로 표시됩니	<u>조치 방법 상세 안내</u>
		Ψ

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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. <u>보안 점검</u>을 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.

AhnLab LIPC XI7[0]					
HOME PC 점검	페스워드 점검 도구	PC 최적화	보고서		
점검 내용			🔺 i	점검 점수 <mark>: 85</mark> 점	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 - 로필 보안 정책 점검 - 너트워크 설정 점검	▲ 향목 ▼ 바이러스 백신 설 바이러스 백신의 운영 체제, MS Of 한글 프로그램의	치 및 실행 점검 최신 보안 패치 점검 fice 최신 보안 패치 최신 보안 패치 점검	점겸	2	과 · · · · · · · · · · · · · · · · · · ·
점겸 항목 상세 정보 점겸 결과: 안전				*	
PC의 한글 프로그램이 최신 상	태입니다.				
				<u>ح</u>	<u>치 방법 상세 안내</u>

- 4. 항목의 한글프로그램의 최신 보안 패치 점검을 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 설치하기를 눌러 최신 보안 패치를 적용하십시오.
 - 점검 불가: 한글 프로그램의 최신 보안 패치 적용 여부를 확인할 수 없는 경우입니다.

한 한 고

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

조치 방법

• <u>한글 프로그램의 최신 보안 패치 점검</u>

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

한참고

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.

패스워드 안전성 검사 - AhnLab 내PC지키미	×
패스워드 안전성 검사를 위해 Windows의 패스워드를 입력하십시오.	
Windows 로그온 패스워드를 입력하십시오.	
확인 취소	

한참고

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

- 2. <u>보안 점검</u>을 실행하여 점검 결과를 확인합니다.
- 3. 점검 완료 창을 닫은 후 내PC지키미의 PC 점검 탭을 선택합니다.
- 점검 내용의 기본 취약점 점검 목록 > 패스워드 안전성 검사에서 로그온 패스워드 안전성 점검을 선택 합니다.

🛃 AhnLab ЦРС⊼(₹ □					_ D X
HOME PC 점검	피스위드 점검 도구	PC 최적화	보고서		
점겸 내용			A	점검 점수 : 85점	점감 시작
전체 점겸 목록 기본 취약점 점겸 목록 보안 업데이트 - 패스위드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 보인 프로그램 설치 - 관리자 추가 점검 확장 취약점 점겸 목록 - Windows 설정 점겸 - 계정 설정 점겸 - 로럴 보안 정책 점겸 - 네트워크 설정 점겸	▲ 항목 ▼ 로그온 패스워드 로그온 패스워드	안전성 점검 사용 기간 점검		21	바 · · · · · · · · · · · · · · · · · · ·
점겸 항목 상세 정보					
점경 결과: 안전 PC가 다음 4개의 항목에 대 1, 로그온 패스워드를 사용하 2, 로그온 패스워드가 사용가 3, 로그온 패스워드가 다음 1 - 9자 이상 4, 패스워드 점검 결과, 패스	해 점검 결과가 '안전'으로 : 하고 있는지 점검합니다. 자 계정과 동일한지 점검합니 패스워드 설정 규칙에 따라 2워드 등급이 '중' 이상인지	판정되었습니다. I다. 설정되었는지 점검험 점검합니다.	HLICH.	*	
					치 방법 상세 안내

- 5. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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. <u>보안 점검</u>을 실행하여 점검 결과를 확인합니다.
- 2. 점검 완료 창을 닫은 후 내PC지키미의 PC 점검 탭을 선택합니다.
- 점검 내용의 기본 취약점 점검 목록 > 패스워드 안전성 검사에서 로그온 패스워드 사용 기간 점검을 선 택합니다.

AhnLab ЦРС⊼ ₹ □					
HOME PC 점검	피스워드 점검 도구	PC 최적화	보고서		
점겸 내용			🛕 :	점검 점수 : 85점	점감 시작
전체 점검 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스위드 안진성 검사 - 화면 보호기 설정 - 공유 폴더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 고럴 보안 정책 점검 - 로럴 보안 정책 점검	▲ 향목 ▼ 로그온 패스워의 로그온 패스워의	E 안진성 점겸 E 사용 기간 점겸		21	▶ ▼ 안전 안전
점겸 항목 상세 정보					
정경 결과: 안진 PC에 최근 90일 이내에 변경	경된 로그온 패스워드가 설	정되어 있습니다.		*	el Harali de la Ofrij
				*	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 변경을 눌러 현재 사용 중인 패스워드를 변경하시기 바랍니다.

조치 방법

• <u>로그온 패스워드 사용 기간 점검</u>

화면 보호기 설정

화면 보호기 설정 점검

화면 보호기 설정에서는 사용자 PC의 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. <u>보안 점검</u>을 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.

AhnLab LIPCX[7][]						
HOME PC 점검	피스위드 점검 도구	PC 최적화	보고서			
점겸 내용			🔺 🔒	점검 점수 : 85점	점검 시작	
전체 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 하면 보호기 설정 - 공유 홀더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 휘약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로컬 보안 정책 점검 - 네트워크 설정 점검	▲ 한목 ▼ 화면 보호기 설정	점검		22	▼	
점검 항목 상세 정보				*		
점검 물과: 안전 화면 보호기가 다음 3가지 (1, 화면 보호기가 설정되어 2, 화면 보호기의 대기 시간 3, 화면 보호기의 암호가 설	방목의 안전 기준을 만족합니 있는지 점검합니다. f미 10분 이하로 설정되어 있 정되어 있는지 점검합니다.	I다. 문는지 점검합니다.				
				- <u>21</u>	<u>() 방법 상세 안내</u>	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 설정을 눌러 화면 보호기를 설정하시기 바랍니다.
- 점검 불가: 화면 보호기 설정 여부를 확인할 수 없는 경우입니다.

조치 방법

• <u>화면 보호기 설정 점검</u>

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. <u>보안 점검</u>을 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.

Z AhnLab LIPC X I 7 [0]						
HOME PC 점검	피스위드 점검 도구	PC 최적화	보고서			
점겸 내용			A :	점검 점수 : 85점	점감 시작	
전체 점경 목록 기본 취약점 점경 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 하면 보호기 설정 - 공유 졸더 설정 - 보안 프로그램 설치 - 관리자 추가 점경 확장 취약점 점경 목록 - Windows 설정 점경 - 로럴 보안 정책 점경 - 너트워크 설정 점경	▲ 한목 ▼ 사용자 공유 폴더	i 설정 점검		21	¥ ▼ 안전	
점겸 항목 상세 정보						
점경 결과: 안전 PC에 사용자 공유 폴더가 성	별정되어 있지 않습니다.			*		
				<u>ع</u> ن	<u>치 방법 상세 안내</u>	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: 사용자 공유 폴더가 설정되어 있지 않은 경우입니다.
 - 취약: 사용자 공유 폴더가 설정되어 있는 경우입니다. 점검 결과가 취약인 경우에는 공유 폴더
 해제하기를 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. <u>보안 점검</u>을 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.

🛛 AhnLab 내PC지키미 💿 🔲 💌						
HOME PC 점검	파스워드 점검 도구	PC 최적화	보고서			
점검 내용			🔺 🔒	점검 점수 <mark>: 85</mark> 점	점검 시작	
전체 점검 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 폴더 설정 - 모인 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로릴 보안 정책 점검 - 너트 위크 선정 적건	▲ 한목 ▼ USB 자동 실역 미사용 Activi	행 설정 점검 xx 프로그램 점검			과 * 안전 취약	
점겸 항목 상세 정보				*		
점겸 결과: 안전 USB 메모리를 PC에 연결했을 때, USB 메모리에 저장된 파일이 자동으로 실행되지 않도록 설정되어 있습 니다. * USB 자동 실행을 사용하면 USB에 저장된 감염 파일을 통해 PC가 약성코드에 감염될 위험이 높아집니 다.				보다에 있습 높아집니 조	<u>치 방법 상세 안내</u>	
				•		

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



• <u>USB 자동 실행 설정 점검</u>

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. <u>보안 점검</u>을 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.

🛃 AhnLab LiPCX 7 0 💷 🔤 🔤 🌌						
HOME PC 점겸	페스워드 점검 도구	PC 최적화	보고서			
점겸 내용			🔺 :	점검 점수 <mark>: 85</mark> 점	점감 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 - 로럴 보안 정책 점검 - 너트워크 설정 점검	▲ 향목 ▼ USB 자동 실행 설 미사용 ActiveX 프 ■	1정 점검 프로그램 점검		2	과 ▼ 안전 취약	
점겸 항목 상세 정보						
점경 결과: 취약 PC에 90일 이상 사용하지 않은 ▶ [ActiveX 삭제하기]를 놀리	: ActiveX 프로그럼이 1개 레 아래 ActiveX 프로그램	! 있습니다. 을 삭제하십시오.		Â	ActiveX 삭제하기	
1. INIwallet61 Control * 위 취약 항목에 대한 후속 조; 니다. * ActiveX 프로그램이 삭제되지	치 후, 보안 점검을 한번 [] 않는 경우, 조치 방법 싱	더 수행하며 PC의 인 상세 안내 > FAQ를 칠	안정성을 최종 점검하 참고하십시오.	시기 바랍 - 조	<u>치 방법 상세 안내</u>	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 삭제하기를 눌러 ActiveX 프로그램 목록에서 관리자가 설정한 기간
 이상 사용하지 않은 ActiveX 프로그램을 삭제해야 합니다.

조치 방법

• <u>미사용 ActiveX 프로그램 점검</u>

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 점검을 선택합니다.

🔽 AhnLab นูPC지키미						
HOME PC 점검	파스	워드 점검 도구	PC 최적화	보고서		
점겸 내용				🔺 🔒	됔검 점수 <mark>: 85</mark> 점	점검 시작
전체 점검 목록	-	항목 포			긜	과 =
기본 취약점 점검 목록		PDF 프로그램의	최신 보안 패치 점검			안전
보안 업데이트 패스이드 야정성 것 #		편집 프로그램 설	치 점검			안전
- 최근 보호기 설정		무선 런카드 설치	점검			안전
- 공유 폴더 설정	=	보안 USB 설치 점	12			안전
		비인가 프로그램	쓸지 삼감			취약
확장 취약점 점검 목록						
Windows 설정 점검						
- 게영 열양 임임 - 로컬 보안 정책 점검						
네트워크 설정 점검	-					
전건 하모 사내 전보						
					*	
점검 결과: 안전						
PC에 설치된 PDF 프로그램(PC에 설치된 PDF 프로그램이 최신으로 업데이트되어 있습니다.					
					3	치 방법 상세 안내
					÷	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab LHPCX 7 0							
номе рс	점겸	파스	워드 점검 도구	PC 최적화	보고서		
점검 내용					🔺 🔒]] 점 점 수 <mark>: 85</mark> 점	점감 시작
전체 점검 목록		-	향목 포			78	과 *
기본 취약점 점검	목록		PDF 프로그램의	최신 보안 패치 점검			안전
- 보안 업데이트	M 71 U		편집 프로그램 설	치 점검			안전
- 패스쿼트 런션	· 최근계드 인건용 답사 · 화면 보호기 설정 · 공유 홀더 설정 · 보안 프로그램 설치 · 관리자 추가 정경 확장 취약점 정경 목록		무선 랜카드 설치	점겸			안전
- 공유 폴더 설정		=	보안 USB 설치 점	12			안전
보안 프로그램			비인가 프로그램	설지 섬겸			취약
확장 취약점 점검							
Windows 설정	! 점검	-					
- 계성 설성 심검] [점검						
- 네트워크 설정	점검	-					
저기 하모 사내 저너							
88 94 84 85	5					*	
점검 결과: 안전							
PC에 허용된 편집	프로그램면	한 설치되	리어 있습니다.				
						2	조 <u>치 방법 상세 안내</u>
						Ŧ	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 삭제하기를 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. <u>보안 점검</u>을 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.

AhnLab LIPCXI71					
HOME PC 점검	페스워드 점검 도구	PC 최적화	보고서		
점겸 내용			A :	점검 점수 : 85점	점감 시작
전체 점검 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 폴디 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 고령 보안 정책 점검	▲ 향목 ▼ PDF 프로그램의 편집 프로그램 설 무선 편가드 설치 보안 USB 설치 점 비인가 프로그램	최신 보안 폐치 점겸 [치 점겸 [점겸 성겸 설치 점겸			▼ 안전 안전 안전 안전 기약
는 네트워크 열정 점점 점겸 항목 상세 정보	•			*	
점검 결과: 안전 PC에 설치된 무선 랜카드가 없; * 무선 랜카드 사용시에 외부로	습니다. 8부터 바이러스가 유입될	성 수 있습니다.			
				- 21	<u>() 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: 사용자 PC 에 무선 랜카드가 설치되어 있지 않습니다.
 - 취약: 사용자 PC 에 무선 랜카드가 설치되어 있습니다. 원클릭 조치를 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

• <u>무선 랜카드 설치 점검</u>

보안 USB 설치 점검

관리자가 설정한 보안 USB 의 설치 정보를 점검합니다.

점검 방법

보안 USB 설치 점검 방법은 다음과 같습니다.

- 1. <u>보안 점검</u>을 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 점검을 선택합니다.

HOME PC 점검	피스	위드 점검 도구	PC 최적화	보고서		•
점겸 내용				A	점검 점수 <mark>: 85</mark> 점	점검 시작
전체 정경 목록	^	향목 🔻			ī	결과 포
기본 취약점 점검 목록		PDF 프로그램의	최신 보안 패치 점검			안전
- 보안 업데이트		편집 프로그램 설치 점검				안전
- 패스워드 안선성 검사 - 하면 보호기 설정		무선 런카드 설치	점검			안전
- 공유 폴더 설정	=	보안 USB 설치 질	경검			안전
보안 프로그램 설치		비인가 프로그램	설치 점겸			취약
·····································	· 관리사 추가 점검 장 취약점 점검 목록					
- Windows 설정 점검						
- 계정 설정 점검 그러 비아 저해 저겨						
- 네트워크 설정 점검	+					
저기 하무 사내 저너						
저거 견규·아저					*	
86 24- 20						
PC에 관리자가 지정한 보인	한 USB가	모두 설치되어 있습	LICH.			
					1	<u>조치 방법 상세 안내</u>
					Ŧ	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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

• <u>보안 USB 설치 점검</u>

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. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab LIPCX[7]0]						
HOME PC 점검	피스	워드 점검 도구	PC 최적화	보고서		
점겸 내용				🔺 🔒	점검 점수 <mark>: 85</mark> 점	점감 시작
전체 점검 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 폴더 설정 - 보안 프로그램 설치		항목 * PDF 프로그램의 편집 프로그램 설 무선 렌카드 설치 보안 USB 설치 정 비인가 프로그램	최신 보안 패치 정겸 치 정경 정경 경검 설치 정경		1	과 ▼ 안전 안전 안전 안전 취약
- 관리자 추가 점경 확장 취약점 점경 목록 - Windows 설정 점경 - 계정 설정 점경 - 로컬 보안 정책 점경 - 네트워크 설정 점경						
점겸 항목 상세 정보						
점검 결과: 취약 PC에 87개의 비인가 프로그 ▶ [프로그램 삭제하기]를	점검 결과: 취약 PC에 87개의 비인가 프로그램이 설치되어 있습니다. ▶ [프로그램 삭제하기]을 눌러 모든 비인가 프로그램을 삭제하십시오.					프로그램 삭제하기
1. Microsoft Lync - 환영 2. A-Tuning v2.0,116.3 - 3. ASRock App Charger 4. ASRock SmartConnec 5. ASRock XFast RAM v3 6. ATnotes Version 9.5 - 7. Adobe AIR - Adobe Sy 8. Adobe Flash Player 2 9. Abol ab Online Securi	합니다 t v1,0,6 - 3,0,3 - A Thoma: ystems I 1 Active> tu - Abol	- localhost ASRock Inc, - ASRock Inc, SRock Inc, SRock Inc, s Ascher ncorporated < - Adobe Systems Lab. Inc	s Incorporated		<u>,</u>	<u>치 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: 비인가 프로그램이 사용자 PC 에 설치되어 있지 않습니다.
 - 취약: 비인가 프로그램이 사용자 PC에 설치되어 있는 경우로 설치된 비인가 프로그램의 개수와 설치된 프로그램 목록을 보여줍니다. 취약으로 진단된 경우 설치된 비인가 프로그램의 이름을 확인하고 프로그램 삭제하기를 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. <u>보안 점검</u>을 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 점검을 선택합니다.

🛃 AhnLab 내PC지키미						
HOME PC 점검	피스	위드 점검 도구	PC 최적화	보고서		
점겸 내용				A	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 - 료럴 보안 정책 점검	* E	항목 ▼ Windows 자동 업 보안 센터 서비스 사용자 계정 컨트 Windows 이벤트	데이트 설정 점검 실행 정검 롤(UAC) 설정 점검 로그 덮어쓰기 설정	점검	21	바 ▼ 안전 한전 위약 안전
점감 항목 상세 정보	Ŧ					
점검 클과: 안전 PC에 Windows 자동 업데이	비트가 설	정되어 있습니다.			*	
						<u>치 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: Windows 자동 업데이트가 설정되어 있는 경우입니다.
 - 취약: Windows 자동 업데이트가 설정되어 있지 않은 경우입니다. 원클릭 조치를 눌러 Windows 자동 업데이트를 설정하십시오.

조치 방법

• <u>Windows 자동 업데이트 설정 점검</u>

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. <u>보안 점검</u>을 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 점검을 선택합니다.

	14						
номе	PC 점겸	파스	워드 점검 도구	PC 최적화	보고서		•
점검 내용					A	점검 점수 <mark>: 85</mark> 점	점감 사작
전체 정경 목록		-	항목 포			ī	결과 포
기본 취약점 점	김 목록		Windows 자동 입	법데이트 설정 점검			안전
- 보안 업데이	트		보안 센터 서비스	: 실행 점검			안전
- 패스쿼드 인	- 화면 보호기 설정 - 장면 보호기 설정 - 공유 볼더 설정 - 본안 프로그램 설치 - 관리자 추가 점검 확장 휘약점 점검 목록		사용자 계정 컨트	톨(UAC) 설정 점검			취약
공유 폴더 승		E	Windows 이벤트	로그 덮어쓰기 설정	점겸		안전
- 보안 프로그 과리지 초기							
확장 취약점 점							
Windows	설정 점검						
- 계성 설성 성	임감 영책 정경						
네트워크 설	[정 점검	-					
저겨 하묘 사내 3	ан						
88 84 84 8	530					*	
점검 결과: 안?	<u>M</u>						
PCM Windows	s 보안 센터(\$	Security	Center) 서비스가	실행 중입니다.			
							조 <u>치 방법 상세 안내</u>
						Ŧ	

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

조치 방법

• <u>보안 센터 서비스 실행 점검</u>

사용자 계정 컨트롤(UAC) 사용 점검

사용자 PC에 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 점검을 선택합니다.

Annuab HPCX[7]U				
HOME PC 점검	패스워드 점검 도구 PC 최적화	보고서		
점겸 내용		🛕 점검	점수 : 85점	점검 시작
전체 정경 목록	항목 ▼		결과	Ψ
기본 취약점 점검 목록	Windows 자동 업데이트 설정 점검	(e	t전	
보안 업데이트	보안 센터 서비스 실행 점검		t전	
패스쿼드 안신성 검사 화면 보호기 설정	사용자 계정 컨트롤(UAC) 설정 점검		약	
- 공유 폴더 설정	■ Windows 이벤트 로그 덮어쓰기 설정	점겸		1건
보안 프로그램 설치				
확장 취약점 점검 목록				
- Windows 설정 점검				
계정 설정 점검 				
네트워크 설정 점검	-			
점겸 항목 상세 정보				
점검 결과: 취약			A	·클릭 조치
PC에 사용자 계정 컨트롤(U ▶ [원클릭 조치]를 눌러 /	C)이 설정되어 있지 않습니다. 용자 계정 컨트롤(UAC) 사용을 설정하십시오.			
* 위 취약 항목에 대한 후속 니다.	치 후, 보안 점검을 한번 더 수행하여 PC의 인	·정성을 최종 점검하시기 H	바랍	
			<u>조치</u>	방법 상세 안내

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

조치 방법

• <u>사용자 계정 컨트롤(UAC) 설정 점검</u>

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. <u>보안 점검</u>을 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.

AhnLab LIPCX(7)0					
HOME PC 점검	패스워드 점검 도구	PC 최적화	보고서		
점겸 내용			🔒 (점검 점수 : 85점	점감 시작
전체 점겸 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 관리자 추가 점겸 확장 취약점 점검 목록 - Windows 설정 점검 - 로럴 보안 정책 점검 - 로럴 보안 정책 점검	▲ 항목 ▼ Windows 자동 (보안 센터 서비 사용자 계정 컨트 Windows 이벤트	업데이트 설정 점겸 스 실행 점겸 트롤(UAC) 설정 점겸 트 로그 덮어쓰기 설정	점검	21	▶ ▼ 안전 취약 안전
점검 항목 상세 정보 점검 결과: 안전 Windows 이벤트 로그를 덮	!어쓰지 않도록 설정되어 있	습니다.		*	
				<u></u>	<u>티 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: Windows 이벤트 로그를 덮어쓰지 않도록 설정되어 있는 경우입니다.
 - 취약: Windows 이벤트 로그를 덮어쓰도록 설정되어 있는 경우입니다. 취약으로 진단된 경우, 원클릭
 조치를 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. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab 내PC지키미						
HOME PC 점검	파스	위드 점검 도구	PC 최적화	보고서		
점겸 내용				4	점검 점수 : 85점	점검 시작
기본 취약점 점검 목록	-	항목 ▼			긜	과 🔻
보안 업데이트		Windows 자동 로	그온 점검			안전
- 패스워드 안전성 검사		Administrator 계	정 사용 점겸			안전
- 화면 보호기 설성 - 공은 폭터 석정		사용 안 함 계정 🤄	삭제 점검			안전
보안 프로그램 설치	=	Guest 계정 사용	점겸			안전
관리자 추가 점검	가점겸 패스위		간 제한 설정 점검			취약
확장 취약점 점검 목록		장기간 미접속 계	정 점검			안전
· 개정 설정 정경		패스워드 암호화	알고리즘 설정 점검			안전
로컬 보안 정책 점검		Administrators 그	L룹 내 사용자 계정 A	역겸		안전
네트워크 설정 점검						
는 웹 드라두세 열정 점점						
점겸 항목 상세 정보						
3171 2121 0131					*	
엄마 날봐. 전신						
PC에 Windows 자동 로그	1온이 설정	되어 있지 않습니다				
					*	치 방법 상세 안내

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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

• <u>Windows 자동 로그온 점검</u>

Administrator 계정 사용 점검

사용자 PC 에서 Administrator 계정을 사용하고 있는지 점검합니다.

점검 방법

Administrator 계정 사용 점검 방법은 다음과 같습니다.

- 1. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab LHPC	지키미						
номе	PC 점검	파스	워드 점검 도구	PC 최적화	보고서		
점검 내용					4	점검 점수 : 85점	점검 시작
기보 취약적	정견 목록	^	항목 포			2	과 🔻
- 보안 업(데이트		Windows 자동 로	그온 점검			안전
- 패스워드	: 안전성 검사		Administrator 계종	정 사용 점검			안전
- 화면 보: 고 이 종(호기 설정 리 성제		사용 안 합 계정 🤄	삭제 점검			안전
보안 프	그 글 8 로그램 설치	=	Guest 계정 사용	점겸			안전
- 관리자			패스워드 사용 기간 제한 설정 점검				취약
확장 취약점			장기간 미접속 계	정 점검			안전
계정 설			패스워드 암호화	알고리즘 설정 점검			안전
- 로컬 보	간 정책 점검		Administrators 그	.룹 내 사용자 계정 질	12		안전
- 네트워크	· 설정 점겸 이미 서저 저거						
		-					
점겸 항목 상/	네 정보						
점검 결과:	만전					^	
PCM Admi	nistrator계정 시	J용이 설	형되어 있지 않습니!	Cł.			
						_ 3	치 방법 상세 안내
						•	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: PC 에 Administrator 이름의 계정이 존재하지 않습니다.
 - 취약: PC 에 Administrator 이름의 계정이 존재합니다. 원클릭 조치를 눌러 Administrator 계정 이름을 변경하십시오.

조치 방법

• <u>Administrator 계정 사용 점검</u>

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. <u>보안 점검</u>을 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.

AhnLab 내PC지키미					
HOME PC 점검 패	스위드 점검 도구	PC 최적화	보고서		۰
점겸 내용			A	점검 점수 : 85점	점검 시작
기본 취약점 점검 목록	_ 항목 ▼			결과	7
- 보안 업데이트	Windows 자동 로	그온 점검			안전
패스워드 안전성 검사	Administrator 계	정 사용 점검			안전
화면 모호기 설성	사용 안 함 계정 🤄	삭제 점검			안전
보안 프로그램 설치	트 Guest 계정 사용	점겸			안전
관리자 추가 점검	패스워드 사용 기	간 제한 설정 점검			취약
확장 취약점 점검 목록 	장기간 미접속 계	정 점검			안전
계정 설정 점검	패스워드 암호화	알고리즘 설정 점검			안전
- 로컬 보안 정책 점검	Administrators 그	L룹 내 사용자 계정 질	병경		안전
네트워크 설정 점검 의 브리오퍼 서저 저거					
	- I				
점겸 항목 상세 정보					
정경 결과: 안전				*	
DCM 내용 야 하 계정이 주겠는다					
우니에 사용 한 할 계정이 존재하지	이 않습니다.				
				<u>조</u> 2	<u>() 방법 상세 안내</u>
				Ŧ	

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

조치 방법

• <u>사용 안 함 계정 점검</u>

Guest 계정 사용 점검

사용자 PC 에서 Guest 계정을 사용하는 지 점검합니다.

점검 방법

Guest 계정 사용 점검 방법은 다음과 같습니다.

- 1. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab 내PC지키미						
HOME PC 점검	파스	워드 점검 도구	PC 최적화	보고서		
점겸 내용					점검 점수 : 85점	점검 시작
기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사	, Î	향목 ▼ Windows 자동 로 Administrator 계3	2그온 점경 및 사용 정경		23	안전 안전
화면 보호기 설정 공유 폴더 설정		사용 안 함 계정 《 Guest 계정 사용	삭제 점검 적건			안전
보안 프로그램 설지 관리자 추가 점검 확장 취약점 점검 목록		패스워드 사용 기 장기간 미접속 계	간 제한 설정 점검 정 점검			취약
Windows 설정 점겸 개정 설정 점겸 로컬 보안 정책 점겸		패스워드 암호화 Administrators 그	알고리즘 설정 점검 룹 내 사용자 계정 점	검		안전 안전
네트워크 설정 점검 웹 브라우저 설정 점령	ä +					
점겸 항목 상세 정보						
점검 결과: 안전 PC에 Guest계정 사용이	설정되어	있지 않습니다.			*	
						<u>치 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 함으로 설정하거나 원클릭 조치를 눌러 Guest 계정 이름을 변경하십시오.

조치 방법

• <u>Guest 계정 사용 점검</u>

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

🔀 AhnLab ЩPC⊼(₹ □					- C - X
HOME PC 점검 쾨	스위드 점검 도구	PC 최적화	보고서		
점검 내용			🔺 i	점검 점수 <mark>: 85</mark> 점	점감 시작
전체 점경 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 - 관리 나아 정체 정격	한목 ♥ Windows 자동 5 Administrator 계 사용 안 합 계정 Guest 계정 사용 패스워드 사용 7 장기간 미접속 계 패스워드 암호화 Administrators 그	2 그 온 정경 정 사용 정경 삭제 정경 정경 1간 제한 설정 정경 1정 정경 알고리즘 설정 정경 1를 내 사용자 계정 2	8 7 3		발과 · · · · · · · · · · · · · · · · · · ·
- 네트워크 설정 점검 ·	-				
점검 영국 경제 중도 점검 결과: 취약 PC에 패스워드 사용 기간이 설정되 ▶ [원클릭 조치]를 눌러 계정에 myson + 위 취약 항목에 대한 후속 조치 : 니다.	리지 않은 1개의 계정) 패스워드 사용 기간을 후, 보안 점검을 한번	이 있습니다. § 설정하십시오. 더 수행하며 PC의 인	안정성을 최종 점검하	시기 바람	원클릭 조치
					조 <u>치 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 조치를 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. <u>보안 점검</u>을 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.

AhnLab 내PC지키미						
HOME PC 점검	피스	워드 점검 도구	PC 최적화	보고서		
점겸 내용				4	점검 점수 : 85점	점감 시작
전체 점검 목록	전체 점검 목록 ^ 기본 취약점 점검 목록 · - 보안 업데이트 - 패스워드 안전성 검사 - 화면 보호기 설정 = - 공유 플더 설정 =	항목 ▼			23	1
기본 취약점 점검 목록		Windows 자동 로	은그온 점검			안전
보안 업데이트 패스인드 아저서 거		Administrator 계	정 사용 점검			안전
- 화면 보호기 설정		사용 안 함 계정	삭제 점검			안전
공유 폴더 설정		Guest 계정 사용	점검			안전
보안 프로그램 설치		패스워드 사용 기	간 제한 설정 점검			취약
확장 취약점 점검 목록		장기간 미접속 계	성 섬검			안전
- Windows 설정 점검	1 L	패스워드 암호화	알고리쯤 열성 점검			안전
- 계정 설정 점검	ч.	Administrators	L를 내 사용사 게임 일	18	-	안전
- 네트워크 설정 점검						
점겸 항목 상세 정보						
점검 결과: 안전					^	
PC에 장기가 미정승하	계정이 조재?	하지 않습니다.				
	1801 EAR	in the city.				
					<u> </u>	치 방법 상세 안내
					÷	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: 장기간 동안 접속하지 않은 계정이 존재하지 않는 경우입니다.
 - 취약: 장기간 동안 접속하지 않은 계정이 존재하는 경우입니다. 취약으로 진단된 경우, 원클릭
 조치를 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. <u>보안 점검</u>을 실행하여 점검 결과를 확인합니다.
- 2. 점검 완료 창을 닫은 후 내 PC 지키미의 PC 점검 탭을 선택합니다.
- 점검 내용의 확장 취약점 점검 목록 > 계정 설정 점검에서 패스워드 암호화 알고리즘 설정 점검을 선택합니다.

AhnLab LIPCX(7)0			
HOME PC 점검	페스워드 점검 도구 PC 최적회	보고시	.0.▲
점겸 내용		🛕 점검 점수 : 85점	점검 시작
전체 점검 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 호면 보호기 설정 - 공유 졸ር1 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 로럴 보안 정책 점검 - 네트워크 설정 점검	한목 ▼ Windows 자동 로그온 점검 Administrator 계정 사용 점검 사용 안 함 계정 삭제 점검 Guest 계정 사용 점검 패스워드 사용 기간 제한 설정 점 장기간 미접속 계정 점검 패스워드 암호화 알고리즘 설정 Administrators 그룹 내 사용자 계	2 2 지 · · · · · · · · · · · · · · · · · · ·	과 ▼ 안전 안전 안전 안전 안전 안전 안전
점겸 항목 상세 정보 점겸 결과: 안전 PC의 패스워드 보안 설정이	AN Manager 해시 값을 저장하지 않도록	설정되어 있습니다.	<u> 또치 방법 상체 안내</u>

- 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 조치를 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. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab LIPCX[7]0]						
HOME PC 점검	파스	워드 점검 도구	PC 최적화	보고서		
점겸 내용				🔺 🔒	절검 점수 <mark>: 85</mark> 점	점감 시작
전체 점검 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 출더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검	E	항목 ▼ Windows 자동 로 Administrator 계 사용 안 함 계정 ← Guest 계정 사용 패스워드 사용 기 장기간 미접속 계 패스워드 암호화	2 그온 정경 정 사용 점경 삭제 점경 점경 간 제한 설정 점경 정 점경 알고리즘 설정 점경		22	♥전 안전 안전 안전 안전 안전 안전 안전
개정 설정 정경 로컬 보안 정책 점겸 네트워크 설정 점겸	Ŧ	Administrators	L룹 내 사용자 계정 (엄검		안전
점검 항목 상세 정보 점검 결과: 안전 PC의 Administrators 그룹(에 허가도	I지 않은 사용자 계정	영이 존재하지 않습L	ICł.	<u>م</u>	치 방법 상세 안내
					Ŧ	

- 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 조치를 눌러 Administrators 그룹에 허가되지 않은 사용자 계정을 삭제하십시오.

조치 방법

• <u>Administrators 그룹 내 사용자 계정 점검</u>

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.
- 점검 내용의 확장 취약점 점검 목록 > 로컬 보안 정책에서 Windows 로그온 실패 횟수 초과 시 계정 잠금 설정 점검을 선택합니다.

🛃 AhnLab ЦРС⊼ ヲ □					
HOME PC 점검 패	스위드 점검 도구	PC 최적화	보고서		
점겸 내용			🔺 i	점검 점수 <mark>: 85</mark> 점	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 - 계정 설정 점검	▲ 한목 ♥ Windows 로그온 최근 사용한 패스 패스워드 최대/최	실패 횟수 초과 시 워드 사용 점경 소 사용 기간 설정 (계정 잠금 설정 점검 험검	2	과 * 취약 취약
네트워크 설정 점검 ·	•			*	
점 김 결과: 취약 PC에 Windows 로그온 실패 횟수 ▶ [원클릭 조치]를 눌러 계정 짐	초과 시 계정 잠금이 : 금을 설정하십시오.	설정되어 있지 않습	LICH.		원클릭 조치
* 위 취약 항목에 대한 후속 조치 3 니다.	후, 보안 점검을 한번 [크 수행하여 PC의 인	안정성을 최종 점검하	시기 바람	치 방법 상세 안내
				Ŧ	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: Windows 로그온 실패 횟수 초과 시 계정 잠금이 설정된 경우입니다.
 - 취약: Windows 로그온 실패 횟수 초과 시 계정 잠금이 설정되지 않은 경우입니다. 취약으로 진단된
 경우 원클릭 조치를 눌러 Windows 로그온 실패 횟수 초과 시 계정 잠금이 되도록 설정해야 합니다.

조치 방법

• <u>Windows 로그온 실패 횟수 초과 시 계정 잠금 설정 점검</u>

최근 사용한 패스워드 사용 점검

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

점검 방법

- 1. <u>보안 점검</u>을 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 점검을 선택합니다.

Ə AhnLab 내PC지키미					
HOME PC 점검	패스워드 점검 도구	PC 최적화	보고서		
점겸 내용			🛕 2	점검 점수 <mark>: 8</mark> 5점	점감 시작
전체 점검 목록 기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 최면 보호기 설정 - 공유 출더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로컬 보안 정책 점검	▲ 향목 ▼ Windows 로그 최근 사용한 피 패스워드 최대	온 실패 횟수 초과 시 네스워드 사용 점겸 /최소 사용 기간 설정	계정 잠금 설정 점겸 점겸		철과 · · · · · · · · · · · · · · · · · · ·
	•			*	
점검 결과: 취약 PC에 최근 사용한 패스워드 ▶ [원클릭 조치]를 눌러 :	: 사용 여부를 점검하도록 최근 사용한 패스워드를 /	설정되어 있지 않습니 위장하도록 설정하십시	다. 오.		원클릭 조치
* 위 취약 항목에 대한 후속 니다.	조치 후, 보안 점검을 한	변 더 수행하며 PC의 9	안정성을 최종 점겹하	시기 바랍	조치 방법 상체 안내
				Ŧ	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 조치를 눌러 최근 사용한 패스워드를 저장하도록 설정해야 합니다.

조치 방법

• <u>최근 사용한 패스워드 사용 점검</u>

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. <u>보안 점검</u>을 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 점검을 선택합니다.

🛃 AhnLab 내PC지키미					- C - X
HOME PC 점검	파스위드 점검 도구	PC 최적화	보고서		
점겸 내용			🔥 2	됔검 점수 <mark>: 85</mark> 점	점감 시작
전체 점경 목록 기본 취약점 점경 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 ▼ Windows 로그온 최근 사용한 패스 패스워드 최대/최	: 실패 횟수 초과 시) :워드 사용 점겸 :소 사용 기간 설정 (계정 잠금 설정 점검	2	과 ▼ 취약 취약
점겸 항목 상세 정보				*	
점검 결과: 취약 PC의 암호 정책에서 패스워 ▶ [원클릭 조치]를 눌러 I	드 사용 기간이 설정되어 있 패스워드의 최대/최소 사용	!지 않습니다. 기간을 설정하십시오	<u>≥</u> .		원클릭 조치
* 위 취약 항목에 대한 후속 니다.	조치 후, 보안 점검을 한번	더 수행하며 PC의 9	안정성을 최종 점검하	시기 바랍 - 조	<u>치 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 조치를 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. <u>보안 점검</u>을 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 점검을 선택합니다.

& AhnLab 내PC지키미						
HOME PC 점검	파스	워드 점검 도구	PC 최적화	보고서		•
점겸 내용				4	점검 점수 : 85점	점감 시작
기본 취약점 점검 목록	~	항목 ▼			결과 포	<u>^</u>
- 보안 업데이트	가 업데이트 스워드 안전성 검사 편 보호기 설정 유 졸대 설정 티 가 프로그램 설치 티	원격 데스크톱 사	용 점검		(안전	
패스워드 안전성 검		원격 데스크톱 포	트 변경 점검		(안전	
화면 보호기 설정 고은 폭터 성적		Windows 방화벽	사용 점검		(안전	
- 보안 프로그램 설치		Simple TCP/IP 서	비스 실행 점검		(안전	
관리자 추가 점검		웹 서비스 실행 점	겸		(안전	
확장 취약점 점검 목록		FTP 서비스 실행	(안전			
		비인가된 사용자(NULL Session) 접근 제어 점검			(안전	
- 로컬 보안 정책 점검		무선 랜카드 사용 점검			(안전	!
네트워크 설정 점검	3	원격 사용자의 시	스템 공유 디렉터리	접속 가능 점검	(안전	!
- 웹 브라우셔 설성 섬		인터넷 연결 공유	사용 점검		안전	•
점겸 항목 상세 정보						
전건 경과: 아저					*	
BB EAL CC						
PC에 원격 데스크톱 연	결을 허용하/	지 않습니다.				
					조치	방법 상세 안내
					*	

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

조치 방법

• 원격데스크톱사용점검

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

🛛 AhnLab ЦРС⊼ ₹ □						- • ×	
HOME PC 점검	피스	위드 점검 도구	PC 최적화	보고서			
점겸 내용				🔺 i	점검 점수 : 85점	점검 시작	
기보 치약적 정경 모로	^	항목 ▼			결과 🔻	-	
. 보안 업데이트		원격 데스크톱 사	용 점검		- 안전		
패스워드 안전성 검사		원격 데스크톱 포	트 변경 점검		안전		
화면 보호기 설정 고은 폭티 성적		Windows 방화벽	사용 점검		[안전		
- 보안 프로그램 설치	E	Simple TCP/IP 서	비스 실행 점검		[안전		
관리자 추가 점검		웹 서비스 실행 질	경검		[안전		
확장 취약점 점검 목록		FTP 서비스 실행	점경		[안전		
- Windows 설정 점검		비인가된 사용자(NULL Session) 접근	[안전			
- 로컬 보안 정책 점검		무선 런카드 사용	점겸	[안전			
네트워크 설정 점검			원격 사용자의 시	스템 공유 디렉터리	접속 가능 점겸	[안전	
- 웹 브라우셔 설성 점검	-	인터넷 연결 공유	사용 점검		안전	T	
점겸 항목 상세 정보							
점검 결과: 안전					*		
PC의 원경 데스크통 포트가 2	기본 포	트(3389)가 마닌 벼	견퇴 포트로 섭정되(게 있습니다.			
	1	2(333)/1012 2	00 707 501	A Maciel.			
					조치	방법 상세 안내	
					Ŧ		

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

조치 방법

• 원격데스크톱포트변경점검

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 점검을 선택합니다. Abolah LURC TI FIRI

HOME PC 점검	페스워드 점검 도구	PC 최적화	보고서		•
점겸 내용			A :	절검 점수 : 85 점	점겸 시작
기보 칭약적 전건 모로	항목 ▼			결과 🔻	<u>^</u>
- 보안 업데이트	원격 데스크톱 /	사용 점검		- 안전	
패스워드 안전성 검사	원격 데스크통 3	포트 변경 점검		- 안전	
화면 보호기 설정 고 이 폭디 성적	Windows 방화벽	벽 사용 점검		· 안전	
- 보안 프로그램 설치	Simple TCP/IP	서비스 실행 점검		[안전	
- 관리자 추가 점검	웹 서비스 실행	점겸		[안전	
확장 취약점 점검 목록	FTP 서비스 실형	병점검		[안전	
- Windows 열성 점검 - 계정 섬정 정검	비인가된 사용지	비인가된 사용자(NULL Session) 접근 제어 점검			
로컬 보안 정책 점검	명경 무선 편카드 사용 점검			[안전	
네트워크 설정 점검	원격 사용자의 /	시스템 공유 디렉터리	접속 가능 점검	[안전	
웹 브라우저 설정 점검	 인터넷 연결 공유 	유 사용 점검		- 안전	-
점겸 항목 상세 정보					
점겸 결과: 안전				*	
PC에 Windows 방화벽을 시	용하고 있습니다.				
				조치	<u>방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: Windows 방화벽을 사용하도록 설정되어 있습니다.
 - 취약: Windows 방화벽을 사용하고 있지 않습니다. 원클릭 조치를 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. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab ЦPC⊼ ₹ □				
HOME PC 점검 피	스위드 점겸 도구 PC 최적화	보고서		
점겸 내용		🔒 i	절검 점수 : 85점 점검 시작	
기본 취약점 정검 목록 스 보안 업데이트 - 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 폴더 설정 - 보안 프로그램 설치	항목 ▼ 원격 데스크톱 사용 점검 원격 데스크톱 포트 변경 점검 원격 데스크톱 포트 변경 점검 Windows 방화벽 사용 점검 Simple TCP/IP 서비스 실행 점검		결과 ▼ _ ▲ 안전 안전 안전 안전	
 관리자 추가 점검 확장 취약점 점검 목록 - 'Mindows 설정 점검 - 계정 설정 점검 - 로럴 보안 정해 점검 - 네트위크 설정 점검 - 웹 브라우저 설정 점검 	웹 서비스 실행 점검 FTP 서비스 실행 점검 비인가된 사용자(NULL Session) 접근 무선 렌카드 사용 점검 원격 사용자의 시스템 공유 디렉터리 - 이터넷 여결 공유 사용 정검	웹 서비스 실행 점경 FTP 서비스 실행 점경 비인가된 사용자(NULL Session) 접근 제어 점경 무선 랜카드 사용 점경 원격 사용자의 시스템 공유 디랙터리 접속 가능 점검		
점겸 항목 상세 정보				
점겸 결과: 안전 PC에 실행 중인 Simple TCP/IP	세비스가 없습니다.		수 <u>조치 방법 상세 안내</u>	

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

조치 방법

• <u>Simple TCP/IP 서비스 실행 점검</u>

웹 서비스 실행 점검

사용자 PC 에 웹 서비스가 실행 중인지 점검합니다.

점검 방법

웹 서비스 실행 점검 방법은 다음과 같습니다.

- 1. <u>보안 점검</u>을 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 점검을 선택합니다.

S AhnLab ЩPC⊼[考[□]				l	
HOME PC 점검 파스	녹위드 점검 도구	PC 최적화	보고서		
점겸 내용			🔺 i	점검 점수 : 85점 👘 📘	점검 시작
기본 취약점 점검 목록 - 보안 업데이트 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 폴더 설정 - 보안 프로그램 설치 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 로럴 보안 정책 점검 - 로럴 보안 정책 점검 - 웹 브라우저 설정 점검	한목 ▼ 원격 데스크톱 사태 원격 데스크톱 포 Windows 방화벽 Simple TCP/IP 서 웹 서비스 실행 점 FTP 서비스 실행 3 비인가된 사용자(1 무선 랜카드 사용 원격 사용자의 시: 인터넷 연결 공유	용 점검 트 변경 점검 사용 점검 비스 실행 점검 검 검 점검 NULL Session) 접근 점검 스템 공유 디렉터리 사용 점검	제머 점경 접속 가능 점겸	결과 ▼ 안전 안전 안전 안전 안전 안전 안전 안전 안전	
점겸 항목 상세 정보					
점겸 결과: 안전 PC에 살행 중인 웹 서비스가 없습니	JCJ.			수 고치 방법	<u>법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: PC 에 실행 중인 웹 서비스가 없습니다.
 - 취약: PC 에 웹 서비스가 실행 중입니다. 원클릭 조치를 눌러 웹 서비스를 중지하십시오.

조치 방법

• <u>웹 서비스 실행 점검</u>

FTP 서비스 실행 점검

사용자 PC 에 FTP 서비스가 실행 중인지 점검합니다.

점검 방법

FTP 서비스 실행 점검 방법은 다음과 같습니다.

- 1. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab 내PC지키미					
HOME PC 점검 패스	페스워드 점검 도구 PC 최적화				
점겸 내용			🔺 🔒	점검 점수 : 85점	점검 시작
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 - - 게정 설정 점검 - - 고럼 보안 정해 점검 - - 데트위크 설정 점검 - - 웹 브라우저 설정 점검 -	항목 ▼ 원격 데스크톱 사용 점 원격 데스크톱 포트 변 Windows 방화백 사용 Simple TCP/IP 서비스 웹 서비스 실행 점검 FTP 서비스 실행 점검 비인가된 사용자(NULL 무선 런카드 사용 점검 원격 사용자의 시스템 이터넷 여격 교으 사용	경 경 점검 점검 실행 점검 . Session) 접근 공유 디렉터리 정건	제머 점검 접속 가능 점검	결과 또 인 인 인 인 인 인 인 인 인 인 인 인 인 인 인 인 인 인 인	전 전 전 전 전 전 전 전 전 전 전 전 전 전 전 전 전 전 전
점겸 항목 상세 정보					
점검 결과: 안전 PC에 실행 중인 FTP 서비스가 없습	;ШСł.			<u>.</u>	1 방법 상세 안내

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: PC 에 실행 중인 FTP 서비스가 없습니다.
 - 취약: PC 에 FTP 서비스가 실행 중입니다. 원클릭 조치를 눌러 FTP 서비스를 중지하십시오.

조치 방법

• <u>FTP 서비스 실행 점검</u>

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. <u>보안 점검</u>을 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.

AhnLab 내PC지키미						
HOME PC 점 2	김 피스	페스워드 점검 도구 PC 최적화 보고서				
점겸 내용				🔺 i	철검 점수 <mark>: 85</mark> 점	점겸 시작
기보 칭양적 적경 목록		항목 ▼			결과	· .
- 보안 업데이트		원격 데스크톱 사	용 점검		2	전
패스워드 안전성 김	검사	원격 데스크톱 포	트 변경 점검		2	2
화면 보호기 설정 고이 폭더 성정		Windows 방화벽	사용 점검		2	2
보안 프로그램 설치	ti 👘	Simple TCP/IP 서	비스 실행 점검		(e	전
관리자 추가 점검		웹 서비스 실행 점	경검		(2	전
확장 취약점 점검 목록	74	FTP 서비스 실행	점겸		2	17 <u>7</u>
· 계정 설정 점검	8	비인가된 사용자(NULL Session) 접근 제어 점검				1 <u>7</u>
- 로컬 보안 정책 점	검	무선 런카드 사용 점검			2	년전
- 네트워크 설정 점	검	원격 사용자의 시	스템 공유 디렉터리	접속 가능 점겸	2	1 2
는 웹 브라우셔 설정 (11 -	인터넷 연결 공유	사용 점검		2	<u>전</u> -
점겸 항목 상세 정보						
저거 거지 아제					*	
88 24, 20						
PC에 비인가된 사용지	KNULL Sessi	ion)의 접근 제머가	설정되며 있습니다.			
					조 :	치 방법 상세 안내
					-	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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
 조치를 눌러 비인가 사용자에 대한 접근을 허용하지 않도록 설정하십시오.

조치 방법

• <u>비인가 사용자 접근 제어(NULL Session 접근 제어) 점검</u>

무선 랜카드 사용 점검

사용자 PC 에 무선 랜카드를 사용하고 있는지 점검합니다.

점검 방법

무선 랜카드 사용 점검 방법은 다음과 같습니다.

- 1. <u>보안 점검</u>을 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.

HOME PC 점검 표스위드 점검 도구 PC 최적 보고서 ① * ADME 오 전 점 약 · · · · · · · · · · · · · · · · · · ·	중 AhnLab 내PC지키미			
ACT 188 ACT 287 ACT 287 기는 취약점 62 94록 - 보안 20100E - 보안 20100E - 공유 SC 4284 한록 * 결과 * 한국 * 한국 10.125 A 58 823 한전 한전 한전 · 보안 전대 01E - 보안 전대 01E 한국 10.125 A 58 823 한전 한전 한전 · 보안 전대 01E - 보안 전대 428 한지 10.125 A 58 823 한전 한전 한전 한전 한 · 보안 프로그램 설치 · · · · · · · · · · · · · · · · · · ·	HOME PC 점검 패스	워드 점검 도구 PC 최적화	보고시	
기본 취약점 점검 목록 한목 * 결과 * * - 보안 업데이트	점겸 내용		🛕 점검 점수 : 85점 📃 📑	김 시작
점검 향목 상세 정보 점검 결과: 안전 PC에서 무선 전카드를 사용하지 않습니다. 조치 방법 상세 안내	기본 취약점 점검 목록 - 보안 업데이트 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플데 설정 - 모안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로럴 보안 정책 점검 - 네트위크 설정 점검 - 웹 브라우저 설정 점검	한목 * 원격 데스크톱 사용 점검 원격 데스크톱 포트 변경 점검 Windows 방화벽 사용 점검 Simple TCP/IP 서비스 실행 점검 웹 서비스 실행 점검 타TP 서비스 실행 점검 비인가된 사용자(NULL Session) 접근 제대 무선 랜카드 사용 점검 원격 사용자의 시스템 공유 디렉터리 접색	결과 ▼ 안전 안전 안전 안전 안전 안전 안전 안전 안전 안전	E
점검 결과: 안전 PC에서 무선 전카드를 사용하지 않습니다. ^ · · · · · · · · · · · · · · · · · ·	저것 하목 사내 저님	인디가 인물 승규 사용 점점	20	
	점검 결과: 안전 PC에서 무선 전카드를 사용하지 않(àLICH.	▲ <u>조丸 방법 み</u>	세안내

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: PC 에서 무선 랜카드를 사용하지 않습니다.
 - 취약: PC 에서 무선 랜카드를 사용하고 있습니다. 원클릭 조치를 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. <u>보안 점검</u>을 실행하여 점검 결과를 확인합니다.
- 2. 점검 완료 창을 닫은 후 내 PC 지키미의 PC 점검 탭을 선택합니다.
- 점검 내용의 확장 취약점 점검 목록 > 네트워크 설정 점검에서 원격 사용자 인증의 시스템 공유 디렉터리 접속 가능 점검을 선택합니다.

🔀 AhnLab ЦРС⊼[ヲ]□]							
HOME PC 점겸	피스위	워드 점검 도구	PC 최적화	보고서			
점검 내용				A	점검 점수 : 85점	점감 시작	
기본 취약점 점검 목록 - 보안 업데이트 - 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로렐 보안 정책 점검 - 네트워크 설정 점검 에 비라오지 성제 정격	E	항목 ▼ 원격 데스크톱 사 원격 데스크톱 포 Windows 방화벽 Simple TCP/IP 서 웹 서비스 실행 전 FTP 서비스 실행 비인가된 사용자(무선 런카드 사용 원격 사용자의 시	용 점검 트 변경 점검 사용 점검 비스 실행 점검 경검 점검 (NULL Session) 접근 점검 스템 공유 디렉터리	제어 점검 접속 가능 점검	결과 ▼ 안전 안전 안전 안전 안전 안전 안전 안전		
점 김 항목 상세 정보 점 김 결과: 안전 원격 사용자가 시스템 공유	디렉터리(에 접속할 때 인증	여부를 확인하도록	설정되어 있습니다.			
	<u>조치 방법 상세 안내</u> ~						

- 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
 조치를 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 PC의 인터넷 연결 공유 설정이 다른 네트워크 사용자가 에이전트 PC의 인터넷 연결을 공유하여 사용할 수 있도록 설정되어 있는 지 점검합니다.

점검 방법

인터넷 연결 공유 사용 점검 방법은 다음과 같습니다.

- 1. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab LIPCX	ol						
номе	C점검	파스	위드 점검 도구	PC 최적화	보고서		
점김 내용					A :	점검 점수 : 85점 🛛 📒	점검 시작
기본 취약점 점경	김 목록	-	항목 포			결과 ▼	*
보안 업데이!	걸데이트		Simple TCP/IP 서	비스 실행 점검		안전	
- 패스워드 안?	전성 검사 성적		웹 서비스 실행 점	12		안전	
- 공유 폴더 설	<u>콜</u> 8 정		FTP 서비스 실행	점겸		안전	
- 보안 프로그램	램 설치	=	비인가된 사용자(NULL Session) 접근	! 제어 점검	안전	
- 관리자 추가	점겸		무선 런카드 사용	점검		안전	
Windows 설	3 목록 정 점검		원격 사용사의 시	스템 공유 니텍터리	접속 가능 섬겸	안전	
- 계정 설정 점	겸		인터넷 연결 공유	사용 심심		안전	
- 로컬 보안 정	책 점검		hosts 파일 내 비허용 IP 점검			안전	
- 웹 브라우저	성 점점 설정 점검	-	미어용 DN3 월상	22		22	
점겸 항목 상세 정	¥						
적건 결과: 아저						*	
인터넷 연결 송위	~10 당시 달구	1 않고로	· 열장되어 있습니다	t.			
						<u>조치 방법</u>	상세 안내
						Ŧ	

- 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 조치를 눌러 다른 네트워크 사용자가 에이전트 PC 의 인터넷 연결 공유 기능을 사용할 수 없도록 설정하십시오.

조치 방법

• <u>인터넷 연결 공유 사용 점검</u>

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. <u>보안 점검</u>을 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 점검을 선택합니다.

HOME PC 점검	패스위드 점검 도구 PC 최적화 보고서	0,
점김 내용	🔺 🏻	검 점수 : 85점 점검 시작
기본 취약점 점검 목록 - 보안 업데이트 패스워드 안전성 검사 - 화면 보호기 설정 - 오유 폴더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 로컬 보안 정책 점검 - 네트워크 설정 점검 - 웹 브라우저 설정 점검	항목 * Simple TCP/IP 서비스 실행 점검 웹 서비스 실행 점검 웹 서비스 실행 점검 비인가된 사용자(NULL Session) 접근 제어 점검 무선 편카드 사용 점검 친격 사용자의 시스템 공유 디렉터리 접속 가능 점검 인터넷 연결 공유 사용 점검 hosts 파일 내 비허용 IP 점검 비허용 DNS 설정 점검	결과 · · · · · · · · · · · · · · · · · · ·
범김 항목 상세 정보 점겸 결과: 안전 hosts 파일에 허용되지 않은 I	P 주소가 존재하지 않습니다.	^ <u>조치 방법 상세 안내</u>

- 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 조치를 눌러 허용되지 않은 IP 주소를 사용하지 않도록 설정하십시오.

조치 방법

• <u>hosts 파일 내 비허용 IP 점검</u>

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. <u>보안 점검</u>을 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 점검을 선택합니다.

Annlab HPCX[7]U						
HOME PC 점검 피스	위드 점검 도구 🛛	PC 최적화	보고서			
점김 내용			🔺 🔒	점검 점수 : 85점	점검 시작	
기본 취약점 점검 목록 - 보안 업데이트 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 출더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 과정 설정 점검 - 로럴 보안 정책 점검 - 네트위크 설정 점검	한목 * Simple TCP/IP 서비스 웹 서비스 실행 점검 FTP 서비스 실행 점검 비인가된 사용자(NULL 무선 전카드 사용 점검 원격 사용자의 시스템 인터넷 연결 공유 사용 hosts 파일 내 비허용 II 비허용 DNS 설정 점검	실행 점검 . Session) 접근 지 공유 디렉터리 집 점검 IP 점검	에어 점검 1속 가능 점검	결과 ▼ 안전 안전 안전 안전 안전 안전 안전		
· 네트위크 설정 점검 · · · · · · · · · · · · · · · · · ·	비허용 DNS 설정 점검			<u>안전</u>		
네트워크 연결 속성에 허용되지 않은 DNS 서버 주소가 존재하지 않습니다. <u>조치 방법 상세 안내</u>						

- 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 안내를 참고하여 허용되지 않은 DNS 서버 주소를 사용하지 않도록 설정하십시오.

조치 방법

• <u>비허용 DNS 설정 점검</u>

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. <u>보안 점검</u>을 실행하여 점검 결과를 확인합니다.
- 2. 점검 완료 창을 닫은 후 내PC지키미의 PC 점검 탭을 선택합니다.
- 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 IE 종료 시 임시 인터넷 파일 삭제 점 검을 선택합니다.

AhnLab 내PC지키미	Z AhnLab 내PC지키미						
HOME PC 점검 피스	느워드 점검 도구						
점겸 내용			A	점검 점수 : 85점	점검 시작		
- 보안 업데이트	항목 포			2) 2)	라 ㅜ		
패스워드 안전성 검사	IE 종료 시 임시 인	반터넷 파일 삭제 점	검		안전		
- 화면 보호기 설정	IE 사용자 인증 시	자동 로그온 설정	점겸		안전		
- 농유 줄너 열성	IE 신뢰할 수 있는	사이트 목록의 취임	약성 점검		안전		
관리자 추가 점검	IE ActiveX 컨트롤	타운로드 설정 점감	2		안전		
확장 취약점 점검 목록	IE 사용자 이름/임	호 자동 완성 설정	점겸		안전		
	IE 파일 다운로드	사용 점검			취약		
- 개종 물종 명명 - 로컬 보안 정책 점검	IE 종료할 때 검색	기록 삭제 점검			안전		
네트워크 설정 점검	IE ActiveX 컨트롤	및 플러그 인 실행	점겸		취약		
- 웹 브라우지 설정 점검							
- 기타 임감 ·							
점검 항목 상세 정보							
				*			
심김 열과: 안전							
IE 종료 시 임시 파일을 삭제하도록	설정되어 있습니다.						
				*	치 방법 상세 안내		
[

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: IE 종료 시 임시 파일을 삭제하도록 설정되어 있습니다.
 - 취약: IE 종료 시 임시 파일 삭제 설정이 되어 있지 않습니다. 원클릭 조치를 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. <u>보안 점검</u>을 실행하여 점검 결과를 확인합니다.
- 2. 점검 완료 창을 닫은 후 내 PC 지키미의 PC 점검 탭을 선택합니다.
- 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 IE 사용자 인증 시 자동으로 로그온 점검을 선택합니다.

AhnLab UPCXI7ID						
HOME PC 점검 j	파스위드 점검 도구	PC 최적화	보고서			
점겸 내용			🔥 2] [] 접수 <mark>: 85</mark> 점	점검 시작	
- 보안 업데이트 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플로 설정 - 보안 프로그램 설치 관리자 추가 점검	▲ 항목 ▼ IE 종료 시 임시 IE 사용자 인증 / IE 신뢰할 수 있; IE ActiveX 컨트; IE 사용자 이름/	인터넷 파일 삭제 점 시 자동 로그온 설정 는 사이트 목록의 취약 로 다운로드 설정 점금 압호 자동 와성 설정	검 점검 약성 점검 결 정경		안전 안전 안전 안전 안전	
- Windows 설정 점검 - 계정 설정 점검 - 로컬 보안 정책 점검 - 네트워크 설정 점검 - 웹 브라우저 설정 점검 - 기타 점검	IE 파일 다운로드 IE 종료할 때 검석 IE ActiveX 컨트	드 사용 점겸 색 기록 삭제 점겸 롤 및 플러그 인 실행	점겸		취약 안전 취약	
점 검 항목 상세 정보 점검 결과: 안전 Internet Explorer에서 사용자 인	민증 시 자동으로 로그인	하지 않도록 설정되다	배 있습니다.	<u>م</u>	<u>치 방법 상세 안내</u>	

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: IE 에서 사용자 인증 시 자동으로 로그인하지 않도록 설정되어 있습니다.
 - 취약: IE 에서 사용자 인증 시 자동으로 로그인 하도록 설정되어 있습니다. 원클릭 조치를 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. <u>보안 점검</u>을 실행하여 점검 결과를 확인합니다.
- 2. 점검 완료 창을 닫은 후 내 PC 지키미의 PC 점검 탭을 선택합니다.
- 점검 내용의 확장 취약점 점검 목록 > 웹 브라우저 설정 점검에서 IE 신뢰할 수 있는 사이트 목록의 취약성 점검을 선택합니다.

AhnLab 내PC지키미						
HOME PC 점검	파스위	워드 점검 도구	PC 최적화	보고서		
점검 내용				A	점검 점수 : 85점	점검 시작
- 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 - 계정 설정 점검 - 로럴 보안 정책 점검 - 네트워크 설정 점검 - 웹 브라우지 설정 점검 - 기타 점검		항목 ▼ IE 종료 시 임시 9 IE 사용자 인증 시 IE 신뢰할 수 있는 IE ActiveX 컨트롤 IE 사용자 이름/2 IE 파일 다운로드 IE 종료할 때 검색 IE ActiveX 컨트롤	인터넷 파일 삭제 점 자동 로그온 설정 : = 사이트 목록의 취약 로 다운로드 설정 점점 방호 자동 완성 설정 사용 점검 및 기록 삭제 점검 를 및 플러그 인 실행	겸 점겸 약성 점겸 점 점 검 점 검	21	Y ▼ 안전 안전 안전 안전 취약 위약 취약
점겸 항목 상세 정보 점겸 결과: 안전 IE의 신뢰할 수 있는 사이트	목록에 취	비약점이 존재하지	않습니다.		<u>م</u>	지 방법 상세 안내

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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
 조치를 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. <u>보안 점검</u>을 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 점검을 선택합니다.

🛛 AhnLab ҶҎСҲӏ҄҂҄ӏҴ					- • ×
HOME PC 점검	페스워드 점검 도구	PC 최적화	보고서		
점검 내용			A	점검 점수 <mark>: 85</mark> 점	점감 시작
- 보안 업데이트 - 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로컬 보안 정책 점검 - 로컬 보안 정책 점검 - 네트워크 설정 점검 - 11 트워크 설정 점검	한목 ▼ IE 종료 시 임시 IE 사용자 인증 / IE 신뢰할 수 있는 IE ActiveX 컨트를 IE 사용자 이름/ IE 종료할 때 검석 IE ActiveX 컨트를	인터넷 파일 삭제 점 시 자동 로그온 설정 는 사이트 목록의 취약 로 다운로드 설정 점급 암호 자동 완성 설정 든 사용 점겸 색 기록 삭제 점겸 롤 및 플러그 인 실행	검 점경 약성 점검 점 점 검 점 검	3	과 ▼ 안전 안전 안전 안전 안전 양전 양전 하약
점겸 항목 상세 정보					
점검 결과: 안전 PC에 ActiveX 차단 알림 표시를	돌이 설정이 되어 있지 입	부습니다.		<u>م</u>	<u>치 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 조치를 눌러 IE 의 서명된/서명 안 된 ActiveX 컨트롤 다운로드 설정을 확인으로 설정하십시오.

조치 방법

• <u>IE ActiveX 컨트롤 다운로드 설정 점검</u>

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. <u>보안 점검</u>을 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 점검을 선택합니다.

🛃 AhnLab 내PC지키미					
HOME PC 점검 패	스워드 점검 도구	PC 최적화	보고서		
점검 내용			🔒 2	철검 점수 <mark>: 85</mark> 점	점감 시작
- 보안 업데이트 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로럴 보안 정책 점검 - 네트워크 설정 점검 - 웹 브라우저 설정 점검	▲ 항목 ▼ IE 종료 시 임시 3 IE 사용자 인증 시 IE 신뢰할 수 있는 IE ActiveX 컨트릴 IE 자용자 이름/일 IE 파일 다운로드 IE 종료할 때 검색 IE ActiveX 컨트릴	인터넷 파일 삭제 점 이자동 로그온 설정 아이트 목록의 취약 다운로드 설정 점령 아유 완성 설정 사용 점검 이목 삭제 점검 및 플러그 인 실행	검 점검 참 점 점 검 점 검	22	▶ ▼ 안전 안전 안전 안전 안전 안전 아전 하약 취약
점겸 항목 상세 정보 점겸 결과: 안전 IE에서 ID/패스워드 자동 완성을	사용하지 않습니다.			<u>م</u>	<u>리 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: IE 에서 사용자 이름/암호 자동 완성 기능을 사용하지 않습니다.
 - 취약: IE 에서 사용자 이름/암호 자동 완성 기능을 사용하고 있습니다. 원클릭 조치를 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. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab LIPCX(70					
HOME PC 점검 폐소	스위드 점검 도구	PC 최적화	보고서		
점검 내용			🔒 🔒]] 점 점 수 <mark>: 85</mark> 점	점감 시작
부야 없더미트	항목 🔻			21	21 -
- 패스워드 안전성 검사	IE 종료 시 임시 9	인터넷 파일 삭제 점	겸		안전
- 화면 보호기 설정	IE 사용자 인증 사	시 자동 로그온 설정	점겸		안전
- 공유 쓸데 설정	IE 신뢰할 수 있는	는 사이트 목록의 취약	약성 점검		안전
관리자 추가 점검	IE ActiveX 컨트롤	를 다운로드 설정 점령	2		안전
확장 취약점 점검 목록	IE 사용자 이름/일	암호 자동 완성 설정	점겸		안전
Windows 설정 점검	IE 파일 다운로드	사용 점검			취약
- 로컬 보안 정책 점검	IE 종료할 때 검식	백 기록 삭제 점검			안전
네트워크 설정 점검	IE ActiveX 컨트롤	롣 및 플러그 인 실행	점겸	•	취약
- 웹 브라우저 설정 점검 기타 제건					
점겸 항목 상세 정보					
점검 결과: 취약				*	워클린 조치
IE 파일 다운로드가 가능하도록 설 ▶ [원클릭 조치]를 눌러 파일 다	정되어 있습니다. 운로드 설정을 '사용	안 함 으로 설정하습	시오.		00120
* 위 취약 항목에 대한 후속 조치 최 니다.	#, 보안 점검을 한번	더 수행하며 PC의 9	반정성을 최종 점검하	시기 바람	
					<u>치 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: IE 에서 파일 다운로드 설정이 **사용 안 함**으로 설정되어 있습니다.
 - 취약: IE 에서 파일 다운로드 설정이 사용으로 설정되어 있습니다. 취약으로 판단된 경우, 원클릭
 조치를 눌러 해당 기능을 사용 안 함으로 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. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab ЦРС⊼ ₹ □						- • ×
HOME PC 점검	파스	워드 점검 도구	PC 최적화	보고서		
점겸 내용				🔺 i	<u> 점</u> 검 점수 <mark>: 85</mark> 점	점검 시작
- 보안 업데이트 - 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 풀더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 계정 설정 점검 - 로럴 보안 정핵 점검 - 네트워크 설정 점검 - 비트워크 설정 점검	*	항목 ▼ IE 종료 시 임시 \$ IE 사용자 인증 시 IE 신뢰할 수 있는 IE ActiveX 컨트롤 IE 사용자 이름/2 IE 파일 다운로드 IE 종료할 때 검색 IE ActiveX 컨트롤	인터넷 파일 삭제 점 시 자동 로그온 설정 는 사이트 목록의 취약 로 다운로드 설정 점 방호 자동 완성 설정 시용 점검 제 기록 삭제 점검 를 및 플러그 인 실행	검 점검 상성 점검 정 점검 점검		▶ ▼ 안전 안전 안전 안전 안전 안전 한전 하약 취약
점겸 항목 상세 정보						
점겸 결과: 안전 IE 중료할 때 검색 기록을 삭제	1하도:	록 설정되어 있습니[- }.		<u>م</u>	<u>치 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: IE 검색 기록 설정에서 종료할 때 검색 기록 삭제가 선택되어 있습니다.
 - 취약: IE 검색 기록 설정에서 종료할 때 검색 기록 삭제가 선택 해제되어 있습니다. 점검 결과가 취약으로 진단된 경우, 원클릭 조치를 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. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab LIPCX[7]0]						
HOME PC 점검	파스	워드 점검 도구	PC 최적화	보고서		
점검 내용				🔺 🦀 🕯	됔검 점수 <mark>: 85</mark> 점	점감 시작
보안 업데이트	Â	항목 ▼			21	과 포
패스워드 안전성 검사		IE 종료 시 임시 영	인터넷 파일 삭제 점	김		안전
- 화면 모호기 설성		IE 사용사 인증 시	I 사동 로그온 설성 :	섬김		안전
- 보안 프로그램 설치		표 신뢰할 수 있는	E 사이트 목록의 취약	43 22 N	_	안전
- 관리자 추가 점검	=	IE ActiveX 컨트롤	F 나운로드 설성 섬성	3	_	안전
확장 취약점 점검 목록 Windows 성적 정경		IE 사용사 비통/일	Y도 사용 환경 열정	82	-	인전
계정 설정 점검		표 파일 나운도드	사용 임임			위탁
로컬 보안 정책 점검	_	IE 중도걸 때 감색	역 가족 역제 영업 8 미 프리그 이 사해	저건		원인
네트워크 설정 점검		IE ACTIVES 215-3	e x echu 2 eo	88	-	M-R
- 기타 점검	-					
점겸 항목 상세 정보						
점검 결과: 취약					*	워클릭 조치
IE ActiveX 컨트롤 및 플러그 ▶ [원클릭 조치]를 눌러 IE	인 실험 Active	#을 허용하도록 설정 ※ 컨트롤 및 플러그	성되어 있습니다. 인 실행을 '관리자	승인'으로 설정하십시	12.	
* 위 취약 항목에 대한 후속 3 니다.	* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.					
					<u></u>	<u>치 방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 표시됩니다.
 - 안전: IE ActiveX 컨트롤 및 플러그 인 실행의 설정 값이 관리자 승인/사용 안 함/확인으로 설정된 경우입니다.
 - 취약: IE ActiveX 컨트롤 및 플러그 인 실행의 설정 값이 사용으로 설정된 경우입니다. 점검 결과가 취약으로 진단된 경우, 원클릭 조치를 눌러 IE 의 ActiveX 컨트롤 및 플러그 인 실행을 관리자 승인으로 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 PC의 시간을 NTP(Network Time Protocol) 서버와 동기화하는 것을 의미합니다. 즉, 사용자 PC의 시간을 NTP 시간 서버의 시간과 일치하도록 업데이트하여 사용자 PC의 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. <u>보안 점검</u>을 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 점검을 선택합니다.

🛃 AhnLab 내PC지키미						
HOME PC 점검	파스위드 점검	도구 PC최	직화	보고서		
점겸 내용				A	점검 점수 : 85점	점검 시작
- 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로컬 보안 정책 점검 - 네트워크 설정 점검 - 웹 브라우저 설정 점검 - 기타 점검	▲ 향목 ▼ NTP 시: 전체 공 사용자 비 하드디: 소프트위 개인정: 더이터 Adobe	간 서버와 자동 동기 유(Everyone) 권한의 정의 취약점 점검 노크 파일 시스템의 1 데어 저작권 점검 프로 인미처리 파일 개수 실행 방지(DEP) 사용 Flash Player 최신 업 AIR 최신 업데이트 2	화 설정 점감 의 공유 폴더 NTFS 사용 2 로그램 실행 초과 점검 응 점검 데이트 점검 업리 요. 6 00 00	3 사용 점검 점검 점검	결과 ▼ 안전 안전 안전 전점 점점 문 안전 안전 안전	
점경 항목 상세 정보 점경 결과: 안전 PC에 NTP 시간 서버와 자동	· 동기화가 설정되	어 있습니다.			へ <u> 至丸</u>	<u>방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 조치를 눌러 사용자 PC 의 시간이 NTP 시간 서버와 동기화되도록 설정해야 합니다.

조치 방법

• <u>NTP 시간 서버와 자동 동기화 설정 점검</u>

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

AhnLab 내PC지키미		
HOME PC 점검 j	스워드 점검 도구 PC 최적화 5	אם. סי
점검 내용		🛕 점검 점수 : 85점 👘 점검 시작
- 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로컬 보안 정책 점검 - 대트워크 설정 점검 - 웹 브라우저 설정 점검 - 11 드 점 김	 한목 * NTP 시간 서비와 자동 동기화 설정 점검 전체 공유(Everyone) 권한의 공유 폴더 사용 사용자 정의 취약점 점검 하드디스크 파일 시스템의 NTFS 사용 점검 소프트웨어 저작권 점검 프로그램 실행 점검 게인정보 미처리 파일 개수 초과 점검 데이터 실행 방지(DEP) 사용 점검 Adobe Flash Player 최신 업데이트 점검 Adobe AIR 최신 업데이트 점검 	2 관 ♥ ▲ 안전 안전 안전 안전 안전 장경 불가 정경 불가 양전 안전 안전 안전
정경 하목 산세 정보	▼ Java SE Runtime Environment 최신 업데이트	점검 안전 *
점검 결과: 안전 PC에 전체 공유(Everyone) 권한	으로 설정된 공유 톨더가 없습니다.	수 <u>조치 방법 삼세 안내</u> ~

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 해제하기를 눌러 PC 에 설정되어 있는 모든 사용자 공유 폴더를 해제하십시오.

조치 방법

• <u>전체 공유(Everyone) 권한의 공유 폴더 사용 점검</u>

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.

AhnLab ЦРСХ[Я]□]						
HOME PC 점검	페스위드 점검 도구	PC 최적화	보고서			
점검 내용			4	점검 점수 : 85점	점검 시작	
- 패스워드 안전성 검사 화면 보호기 설정 - 공유 풀더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로컬 보안 정책 점검 - 대트워크 설정 점검 - 웹 브라우저 설정 점검 - 기타 점검	▲ 한목 ▼ NTP 시간 서버오 전체 공유(Every 사용자 정의 취역 하드디스크 파일 소프트웨어 저직 개인정보 미처리 데이터 실행 방거 Adobe Flash Pla Adobe AIR 최신	사 자동 동기화 설정 전 one) 권한의 공유 볼 전점 점검 시스템의 NTFS 사용 권 점검 프로그램 실 파일 개수 초과 점검 미(DEP) 사용 점검 yer 최신 업데이트 점 업데이트 점검	점검 더 사용 점검 행 점검 행 검 검	결과 * 안전 안전 안전 전 전 정경 불 정경 불 안전 안전 안전		
점겸 항목 상세 정보	Java SE Runtim	e Environment 최신	입네이트 섬검	224		
점검 결과: 안전 사용자 정의 취약점 점검 항목이 모두 안전 조건을 준수하고 있습니다. ⁴ <u>조치 방법 상세 안내</u>						
				Ŧ		

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 해결하기를 눌러 안전 조건에 따라 취약 서비스의 상태를 변경하십시오. 또는 점검 항목
 상세 정보에 명시되어 있는 안전 조건을 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. <u>보안 점검</u>을 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.

🛃 AhnLab 내PC지키미					- • ×
HOME PC 점검 패	스위드 점검 도구	PC 최적화			
점겸 내용			🔺 i	절검 점수 : 85점 👘	점검 시작
- 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로컬 보안 정책 점검 - 네트워크 설정 점검 - 웹 브라우저 설정 점검 - 기타 점검	항목 ▼ NTP 시간 서버외 전체 공유(Every 사용자 정의 취익 하드디스크 파일 소프트웨어 저작 개인정보 미처리 데이터 실행 방지 Adobe Flash Play Adobe AIR 최신	T 자동 동기화 설정 장 one) 권한의 공유 풀 점 점겸 시스템의 NTFS 사용 권 점겸 프로그램 실 파일 개수 초과 점겸 (DEP) 사용 점겸 er 최신 업데이트 점 업데이트 점겸	성경 더 사용 점경 한 점경 행 점경 응 건	결과 ▼ 안전 안전 안전 안전 점검 불기 안전 안전 안전	
점겸 항목 상세 정보		Environment 212			
점검 결과: 안전 PC의 하드디스크 파일 시스템이 M	NTFS입니다.			수 <u>조치 방</u> *	법 상세 안내

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

조치 방법

• <u>하드디스크 파일 시스템의 NTFS 사용 점검</u>

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. <u>보안 점검</u>을 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 점검을 선택합니다.

Anntab HPCX[7]U		
HOME PC 점검	페스워드 점검 도구 PC 최적화 보고서	
점겸 내용		🚹 점검 점수 : 85점 👘 점검 시작
패스워드 안전성 검사	항목 ▼	결과 ▼
화면 보호기 설정	NTP 시간 서비와 자동 동기화 설정 점검	안전
- 공유 폴더 설정	전체 공유(Everyone) 권한의 공유 폴더 사용 점검	안전
보안 프로그램 설지 	사용자 정의 취약점 점검	안전
확장 취약점 점검 목록	티 하드디스크 파일 시스템의 NTFS 사용 점겸	안전 등
- Windows 설정 점검	소프트웨어 저작권 점검 프로그램 실행 점검	점검 불가
계정 설정 점겸 근컴 보아 저채 저기	개인정보 미처리 파일 개수 초과 점검	점검 불가
- 네트워크 설정 점검	데이터 실행 방지(DEP) 사용 점검	안전
웹 브라우저 설정 점검	Adobe Flash Player 최신 업데이트 점검	안전
- 기타 점검	Adobe AIR 최신 업데이트 점검	안전
	▼ Java SE Runtime Environment 최신 업데이트 점검	안전 ▼
점겸 항목 상세 정보		
전건 경과: 전건 분가		*
00 EV. 00 EV		
> 프로그램을 잘못된 형식으	로 로드하려고 했습니다.	
		조치 방법 상세 안내
		-

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 실행하기를 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.

한참고

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. <u>보안 점검</u>을 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 점검을 선택합니다.

Annlab HPCX[7]U					
HOME PC 점검	페스위드 점검 도구	PC 최적화	보고서		
점겸 내용			A	점검 점수 : 85점	점검 시작
패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 로럴 보안 정책 점검 - 너트워크 설정 점검 - 웹 브라우저 설정 점검 - 웹 브라우저 설정 점검	▲ 향목 ▼ NTP 시간 서비와 전체 공유(Everyo 사용자 정의 취익 하드디스크 파일 소프트웨어 저작 개인정보 미처리 데이터 실행 방지 Adobe Flash Play Adobe AIR 최신	+ 자동 동기화 설정 절 one) 권한의 공유 폴 점 점겸 시스템의 NTFS 사용 권 점겸 프로그램 설립 파일 개수 초과 점겸 (OEP) 사용 점겸 er 최신 업데이트 점 업데이트 점겸	성경 더 사용 점경 한 점경 행 점경 김	2과 ▼ 안전 안전 안전 전 전 경경 5 · · · · · · · · · · · · · · · · · ·	
점겸 항목 상세 정보					
점경 결과: 점경 불가 작업을 완료했습니다.				수 - <u>조치</u>	<u>방법 상세 안내</u>

- 4. 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보가 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 실행하기를 눌러 AhnLab Privacy Management 프로그램에서 처리되지 않은 개인 정보 파일들을 모두 처리하십시오.

한참고

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

조치 방법

• <u>개인 정보 미처리 파일 개수 초과 점검</u>

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. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab ЦРС⊼[考]□]						
HOME PC 점검	패스위드 점검 도구		PC 최적화	보고서		
점검 내용				A	점검 점수 : 85점	점감 시작
- 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로럴 보안 정책 점검 - 네트워크 설정 점검 - 웹 브라우저 설정 점검	E	항목 ▼ NTP 시간 서버와 전체 공유(Everyo 사용자 정의 취약 하드디스크 파일 소프트웨어 저작 개인정보 미처리 데이터 실행 방지 Adobe Flash Play	자동 동기화 설정 장 one) 권한의 공유 볼 점 점검 시스템의 NTFS 사용 권 점검 프로그램 실 파일 개수 초과 점검 (DEP) 사용 점검 er 최신 업데이트 점 억데이트 적건	점검 더 사용 점검 응 점검 행 점검 성 검	결과 ▼ 안전 안전 안전 전 정경 불 안전 안전	
점검 항목 상세 정보	*	Java SE Runtime	Environment 최신	업데이트 정검	안전	
점검 결과: 안전 데이터 실행 방지(DEP) 기능	:을 사용	하도록 설정되어 있	심습니다.		▲ 조치 범	법 상세 안내
					-	

- 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 조치를 눌러 데이터 실행 방지(DEP) 기능을 사용하도록 설정하십시오.

조치 방법

• <u>데이터 실행 방지(DEP) 사용 점검</u>

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. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab 내PC지키미						
HOME PC 점검	패스위드	점검 도구	PC 최적화	보고서		
점김 내용				4	점검 점수 : 85점	점검 시작
- 패스워드 안전성 검사 - 화면 보호기 설정 - 공유 플더 설정 - 보안 프로그램 설치 - 관리자 추가 점검 확장 취약점 점검 목록 - Windows 설정 점검 - 계정 설정 점검 - 로컬 보안 정책 점검 - 네트워크 설정 점검 - 웹 브라우저 설정 점검 - 기타 점검	수 향 N1 전 사 도 하 소 가 대 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	목 TP 시간 서비와 체 공유(Everyo 용자 정의 취약 드디스크 파일 프트웨어 저작; 인정보 미처리 이터 실행 방지 dobe Flash Play dobe AIR 최신	자동 동기화 설정 전 one) 권한의 공유 풀 점 점검 시스템의 NTFS 사용 권 점검 프로그램 살 파일 개수 초과 정검 (DEP) 사용 점검 er 최신 업데이트 점 업데이트 점검	점검 더 사용 점검 용 점검 행 점검 성 검	경과 * 안전 안전 안전 전 전 경경 등 안전 전 전 인전	
점검 항목 상세 정보 점검 결과: 안전 Adobe Flash Player가 최신:	으로 업데이.	트되어 있습니(a.		میں ج	<u>방법 상세 안내</u>

- Adobe Flash Player 최신 업데이트 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보에 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

• <u>Adobe Flash Player 최신 업데이트 점검</u>

Adobe AIR 최신 업데이트 점검

Adobe AIR 가 최신으로 업데이트되어 있는지를 점검합니다.

점검 방법

Adobe AIR 최신 업데이트 점검 방법은 다음과 같습니다.

- 1. <u>보안 점검</u>을 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 점검을 선택합니다.

AhnLab LIPC	지키미							x
HOME	PC 점검	파스	읽드 점검 도구	PC 최적화	보고서			. •
점겸 내용					4	점검 점수 <mark>: 4</mark>	9점 점감 사	나작
- 패스워!	드 안전성 겸사 호기 설정	^	항목 ▼ 전체 공유(Everyo	one) 권한의 공유 폴	더 사용 점검		결과 ▼ 취약	
공유 폴	오기 월종 더 설정		사용자 정의 취익	점 점검			취약	
- 보안 프 관리자	로그램 설치 추가 점검		하드디스크 파일	시스템의 NTFS 사용	용 점검		취약	
확장 취약점	범점검 목록		소프트웨어 저작	권 점검 프로그램 실 피인 게스 총기 제2	행점검		안전	
Window 계정 설	VS 열장 심김 정 점검	=	데이터 실행 방지	파글 개구 조퍼 집원 (DEP) 사용 점겸	i		취약	=
로컬 보	안 정책 점겸 그 서저 저거		Adobe Flash Play		안전			
웹 브리	패트워크 설정 점검 Adobe AIR 최신 업데이트 김 ᅨ 브라우저 설정 점검 Adobe AIR 최신 업데이트 김			업데이트 점검			취약	
기타 집	13		Java SE Runtime	Environment 최신	업데이트 점검		취약	
점감 양속 강 정긴 경과:	체상도					^		
Adobe Air	(x86)가 최신 업	데이트 실	태가 아닙니다. (현	재 버젼: 21,0,0,176)		업데이트 설치히	171
▶ 최신 배	전인 21.0.0.1798	로 업데이!	트하시기 바랍니다.					
* 위 취약 (니다.	양복에 대한 후속	시기 바람						
						-	<u>소지 방법 상세 </u>	<u>201</u>

- Adobe AIR 최신 업데이트 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보에 점검 결과가 표시됩니다.
 - 안전: Adobe AIR 가 최신으로 업데이트되어 있습니다.
 - 취약: Adobe AIR 가 최신 업데이트 상태가 아닙니다. 업데이트 설치하기를 눌러 최신 버전으로 업데이트하시기 바랍니다.

조치 방법

• <u>Adobe AIR 최신 업데이트 점검</u>

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

🛛 AhnLab ЦРС⊼(₹ □					
HOME PC 점검 피스	:위드 점검 도구	PC 최적화	보고서		
점겸 내용			A	점검 점수 : 49점	점감 시작
패스워드 안전성 검사 ^	항목 ▼			결과 포	<u>^</u>
- 화면 보호기 설정	전체 공유(Everyo	one) 권한의 공유 폴	더 사용 점검	취의	
- 공유 폴더 설정	사용자 정의 취약	점 점검		취의	
보안 프로그램 설치 과리지 추가 저것	하드디스크 파일	시스템의 NTFS 사용	8 점검	취의	
확장 취약점 점겸 목록	소프트웨어 저작	권 점검 프로그램 실	행 점검	[안전	
Windows 설정 점검	개인정보 미처리	파일 개수 초과 점검	1	(안전	
- 계정 설정 점검 티	데이터 실행 방지	(DEP) 사용 점검		취의	
- 도글 도한 영역 영업	Adobe Flash Play	er 최신 업데이트 점	검	안전	
- 웹 브라우저 설정 점검	Adobe AIR 최신 업데이트 점	업데이트 점검		취의	
- 기타 점검	Java SE Runtime	Environment 최신	업데이트 점검	취의	
-][-
점겸 항목 상세 정보					
점검 결과: 취약				A	
Java SE Runtime Environment가 ▶ 최신 버젼으로 업데이트하시기 b	최신 업데이트 상태 바랍니다.	가 아닙니다.			이드 을지하기
Java Runtime Environment 8	현재 버전: 8,0,920,1	14 -> 최신 버전: 9,0	, 770, 3		
* 위 취약 항목에 대한 후속 조치 후 니다.	:, 보안 점검을 한번	더 수행하며 PC의 인	·정성을 최종 점겸히	시기 바람	
				<u>.</u> <u>3</u> 1	<u>방법 상세 안내</u>

- Java SE Runtime Environment 최신 업데이트 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보에 점검 결과가 표시됩니다.
 - 안전: Java SE Runtime Environment 가 최신으로 업데이트되어 있습니다.
 - 취약: Java SE Runtime Environment 가 최신 업데이트 상태가 아닙니다. 업데이트 설치하기를 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 사용 하도록 설정해야만 점검 항목으로 나타납니다.

점검 방법

문서 보호 기능 점검 방법은 다음과 같습니다.

- 1. <u>보안 점검</u>을 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 점검을 선택합니다.

🔯 AhnLab 내PC지키미						
HOME PC 점검	파스	워드 점검 도구	PC 최적화	보고서		
점검 내용				A :	점검 점수 <mark>: 52</mark> 점	점경 시작
패스웨드 안전성 검사	*	항목 ▼			결과	* v
- 화면 보호기 설정		사용자 정의 취약	점 점검			취약
- 공유 폴더 설정		하드디스크 파일	시스템의 NTFS 사용	8 점검		취약
보안 프로그램 설치 과리지 추가 제거		소프트웨어 저작	권 점검 프로그램 실	행 점검	<u>점</u>	김 불가
확장 취약점 점검 목록		개인정보 미처리	파일 개수 초과 점검	1		안전
Windows 설정 점검		데이터 실행 방지	(DEP) 사용 점검			취약
계정 설정 점검 고려 나아 저채 저겨	=	Adobe Flash Play	er 최신 업데이트 점	겸		취약
네트워크 설정 점검		Adobe AIR 최신	업데이트 점검			안전
웹 브라우저 설정 점검		Java SE Runtime	Environment 최신	업데이트 점검		안전
- 기타 점검		문서 보호 기능 질	3김			취약
	Ŧ					Ψ.
점김 항목 상세 정보						
정것 격과: 치얀					A	
						프로세스 관리
죄근 30월간 어용되지 않는 (프로세스 개수: 1개)	프도제스	그의 파일 집군을 담	시했습니다.			
탄지 회스·4 경로·C\P	rogram	Files (x86)\Notena	d++\notenad++ ex	a		
BALXTIN SILICIA	- ogiunn	100 (100) (1000)	arr proception read	•	=	
업무용 프로그램은 문서 보회	2 정책의	예외 정책으로 등	록되도록 관리자에게	요청하십시오.		
알 수 없는 프로세스는 [프로	세스 관	리]를 눌러 이름을	변경할 수 있습니다.			
						조치 방법 상세 안내
					Ŧ	

- 4. 문서 보호 기능 점검 항목을 선택하면 화면 아래에 점검 항목 상세 정보에 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 관리를 눌러 이름을 변경할 수 있습니다.

조치 방법

• <u>문서 보호 기능 점검</u>

5장

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 입력란에 점검 대상 패스워드를 입력하고 점검 시작을 누릅니다.

AhnLab 내PC지키미				
HOME PC 점검	페스위드 점검 도구	PC 최적화	보고서	
점김 대상 정보 입력				
패스워드 입력 🛛 ●	•••	점검 시작		
점겸 결과 패스워드 점겸 결과를 표시	합니다.			
[점검 결과] 패스워드 등급 : 취약				
[패스워드 설정 규칙] 길이 : 4 문자 집합 : 1				
[패스워드 취약 항목] 로그온 패스워드의 길이 9 - 9자 이상	는 필수문자 조합이 설정 규칙	벽에 맞지 않습니다.		

- 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.

6장

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.

🛃 AhnLab Ц	PC지키미				
HOME	PC 점검	파스워드 점검 도구	PC 최적화	보고서	۰.
	전체 항목 정리	선택한 5	함목 정리		
# Win ♥ !	ndows 시스템 Mindows 임시 파일 휴지통 비우기	는 삭제			
(전 1 (전 1 (전 1 (전 1) (전 1) (전 1)	1년 역스플로러 인터넷 임시 파일 식 쿠키 삭제 매스워드 자동 완성	낙제 기록 삭제			

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

보안 점검 중 - AhnLab 내PC지키미	
PC 최적화를 시작합니다. 시스템 사양에 따라 시간이 오래 걸릴 수 있습니다.	
Windows 임시 파일 삭제 중 점겸 진행률	20%

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.

AhnLab ЦРС⊼ ₹ □						_ 0	23
HOME PC 점검	패스위드 점	김 도구	PC 최적화	보고서			• 1
운영 체제 정 Windows 7 E	보 nterprise Service I	Pack 1 (7601)		아티바이러: OhnLab V3 E	스 S/W 정보 ndpoint Security 9,0		
안티 스파이의 AhnLab V3 E Windows Def	레이 S/W 정보 ndpoint Security 9 ender	0		개인 방화벽 AhnLab V3 E Windows Fire	s/w 정보 ndpoint Security 9,0 wall		
점검내역 정견날파	제건 제스 [제]	건경과		* 신왕에 실패된	깐 경우, 심김 결과들 5 정견 보고서	분마나 세신종일 지수 견과	SUL.
2015.09.30 14:54:44	58 71	비 전건 한목(56)	i) 경기·아저(32)	ዘ) 최양(23개) 식태	(12 보고서 보기	지승 문의	1
2015.09.30 12:43:44	58 71	에 적건 한목(55) 에 적건 한목(55)	i) 결과:안전(32)	H) 취약(23개) 실패	(0) <u><u><u></u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u>(1)</u>	전송	
2015.09.30 09:20:23	58 전:	에 점검 항목(55개	H) 결과:안전(32)	H) 취약(23개) 실패	(07 보고서 보기	전송	
2015.09.30 09:19:03	58 전:	해 점검 항목(55기	H) 결과:안전(32)	H) 취약(23개) 실패	(07 보고서 보기	전송	
2015.09.30 09:16:55	58 전:	에 점검 항목(55개	1) 결과:안전(32)	ዘ) 취약(23개) 실패	(07 보고서 보기	전송	E
2015.09.30 09:13:43	58 전:	해 점검 항목(55개	1) 결과:안전(32)	H) 취약(23개) 실패	(07 보고서 보기	전송	
2015.09.25 13:10:59	58 전:	에 점검 항목(55기	H) 결과:안전(32)	H) 취약(23개) 실패	(07 보고서 보기	전송	
2015.09.25 10:23:21	58 전:	에 점검 항목(55개	H) 결과:안전(32)	H) 취약(23개) 실패	(07 보고서 보기	전송	
2015.09.24 19:59:00	58 전:	해 점검 항목(55개	H) 결과:안전(32)	H) 취약(23개) 실패	(07 보고서 보기	전송	
2015.09.24 18:41:58	58 전:	헤 점검 항목(55개	H) 결과:안전(32)	H) 취약(23개) 실패	(07 보고서 보기	전송	
2015.09.24 16:53:55	58 전:	해 점검 항목(55개	H) 결과:안전(32)	H) 취약(23개) 실패	(07 보고서 보기	전송	
2015.09.24 16:43:32	62 전:	헤 점검 항목(55기	H) 결과:안전(35)	ዘ) 취약(20개) 실패	(07 보고서 보기	전송	
2015.09.24 16:01:05	61 전:	에 점검 항목(55기	H) 결과:안전(34)	ዘ) 취약(21개) 실패	(07 보고서 보기	전송	
2015.09.24 15:01:59	63 전:	에 점검 항목(55기	H) 결과:안전(35)	ዘ) 취약(20개) 실패	(07 보고서 보기	전송	
2015.09.24 12:45:49	61 전:	에 점검 항목(55기	i) 결과:안전(34)	H) 취약(21개) 실패	(07 보고서 보기	전송	Ŧ

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 정보에서는 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.

김김 시간	2015.09.30 14:54:44		
IP 주소	10000		
사용자 ID	and the second se		
컴퓨터 이름	and the second s		
운명 체제 정보	Windows 7 Enterprise Service	Pack 1 (7601)	
내PC지키미 버전	46.4.2		
바이러스 백신	AhnLab V3 Endpoint Security	9.0	
점검 결과 서버 전송	전송		
HPC지키미 점검 결과 / ^{점검 함목}	점검 점수: 58점		결과
기본 취약점 점검 목록			
바이러스 백신 설치 및 실행 점검			안전
바이러스 백신의 최신 보안 패치 점경	안전		
운영 체제, MS Office 최신 보안 패치 점검			안전
로그온 패스워드 사용 기간 점검			안전
로그몬 패스워드 만전성 점검			안전
화면 보호기 설정 점검			안전
사용자 공유 풀더 설정 점검 취임			
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	1		인전
확장 취약점 점검 목록			
	점검		취약
Administrators 그룹 내 사용자 계정			

8장

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 여부와 바이러스 백신 실행 여부에 대한 상세 결과를 나타냅니다.
 - 바이러스 백신 설치 여부: 설치 안 함으로 나타나면 백신 상태 확인하기를 눌러 관리 센터에 등록된 백신 정보가 있는지 확인합니다.
 - 바이러스 백신 실행 여부: 실행 안 함으로 나타나면 백신 상태 확인하기를 눌러 Windows 관리 센터에서 바이러스 백신이 사용 중으로 표시되는지 확인합니다.

점검 항목 상세 정보

엄금 양국 경제 경도		
점검 결과: 취약 바이러스 백신 설치 여부 - 설치	*	백신 상태 확인하기
바이러스 백신 실행 여부 - <mark>실행 안 함</mark> ▶ 설치된 바이러스 백신을 실행하십시오. 이 데이 데이 데이 드 프로그		
* 위 취약 항복에 대한 후속 소지 후, 보안 섬겸을 한번 더 수행하며 PC의 안성성을 죄송 섬겸하시기 바랍 니다. * 바이러스 백신을 사용 중임에도 점겸 결과가 '취약'으로 판정되는 경우, 조치 방법 상세 안내 > FAQ를 참 ====================================		
고하십시오.		<u>조치 방법 상세 안내</u>

한참고

바이러스 백신이 설치/실행되고 있는데도 보안센터에 표시되지 않는 경우에는 <u>FAQ 1. 바이러스 백신</u> <u>설치 및 실행 점검</u>을 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

- Windows 작업 표시줄의 시작 > 설정 > 제어판을 선택한 후 클래식 보기로 전환을 선택하여 보안 센터를 실행합니다.
- 2. 보안센터에서 바이러스 백신을 선택하여 설치된 바이러스 백신을 확인합니다.
 - 바이러스 백신이 설치되어 있지 않다면 찾을 수 없음으로 표시됩니다.



바이러스 백신이 설치되어 있으나 실행 중이지 않을 경우 사용 안 함으로 표시됩니다. 설치된
 바이러스 백신을 실행하고 실시간 감시를 실행하십시오.



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

Windows Vista

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

👘 Windows 보안 센터		
Windows Update ਆ <u>Windows 방화벽</u> Windows Defender	보안 기능 컴퓨터를 안전하게 보호하려면 다음 네 가지 보안 기능이 설정되었는 확인하십시오. Windows 보안 센터 사용	•지 또는 올바른 상태인지
👮 인터넷 옵션	방화벽	사용 중 🧿 😡
Microsoft 웹 사이트에서 최 신 보안 및 바이러스 정보 보 기	자동 업데이트 사용하는	고 있지 않음 🧿 🕥
보안 센터에서 알림 메시지를 표시하는 방법을 변경	말웨어 방지	설정 확인 💿 🔿
	바이러스 방지 이 컴퓨터에서 바이러스 백신 소프트웨어를 찾지 못했습니다. 사용 가능한 옵션 표시	찾을 수 없음 이 프로그램 찾기(E)
	스파이웨어 및 기타 맬웨어 방지 iiiii Windows Defender의 상태가 최신이 아닙니다. 사용 가능한 옵션 표시	만료됨 ⊙ 중지금 업데이트(U)
	맬웨어 방지 소프트웨어 및 컴퓨터 보안에 대한 자세한 정보	
	기타 보안 설정 보입	안 상태 양호 🧿 😡
참고 항목 백업 및 복원		

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

🐨 Windows 보안 센터		
 Windows Update Windows 방화벽 Windows Defender 	보안 기능 컴퓨터를 안전하게 보호하려면 다음 네 가지 보안 기능이 설정: 확인하십시오. Windows 보안 센터 사용	되었는지 또는 올바른 상태인지
沈 인터넷 옵션	방화벽	사용 중 💿 🕑
Microsoft 웹 사이트에서 최 신 보안 및 바이러스 정보 보 기	자동 업데이트 사람	용하고 있지 않음 🧿 🕞
보안 센터에서 알림 메시지를 표시하는 방법을 변경	말웨어 방지	설정 확인 🗿 🕟
	바이러스 방지 M AhnLab V3 Internet Security 8.00(가) 꺼져 있습니다. 사용 가능한 옵션 표시	사용하고 있지 않음 • 지금 사용하도록 설정(T)
1	스파이웨어 및 기타 맬웨어 방지 iiii Windows Defender의 상태가 최신이 아닙니다. 사용 가능한 옵션 표시	만료됨 🧕 🕅 🕅 만료됨
	맬웨어 방지 소프트웨어 및 컴퓨터 보안에 대한 자세한 정보	
	기타 보안 설정	보안 상태 양호 🧿 🛞
참고 항목 백업 및 복원		

Windows 7

1. 시작 > 설정 > 제어판에서 보기 기준을 작은 아이콘으로 전환하고 관리 센터를 선택합니다.

중 ♥ ♥ ♥ 제어판 ▶ 모든 제이	버판 항목 ▶	 ◄ 제어판 검색
컴퓨터 설정 변경		보기 기준: 작은 아이콘 💌
🏘 BitLocker 드라이브 암호화	✔ Flash Player(32비트)	
🗃 Realtek HD 오디오 관리자	🐻 RemoteApp 및 데스크톱 연결	📑 Windows CardSpace
Windows Defender	🖑 Windows Update	🔗 Windows 방화벽
🐖 개인 설정	🔞 관리 도구	🏲 관리 센터
🔊 국가 및 언어	🚺 글꼴	☞ 기본 프로그램
🔐 날짜 및 시간	🕎 네트워크 및 공유 센터	🔞 동기화 센터
📮 디스플레이	⑦ 마우스	🧼 메일
🔳 문제 해결	📑 바탕 화면 가젯	🐌 백업 및 복원
🌮 복구	🎎 사용자 계정	💶 색 관리
🚨 색인 옵션	💵 성능 정보 및 도구	째 소리
1型 시스템	🗐 시작	🔜 알림 영역 아이콘
🍱 위치 및 기타 센서	🖶 음성 인식	🔂 인터넷 옵션
鼳 인텔® HD 그래픽	🧧 자격 증명 관리자	🐻 자녀 보호
📑 자동 실행	🔔 작업 표시줄 및 시작 메뉴	📇 장치 관리자
📾 장치 및 프린터	🗃 전원 옵션	📟 전화 및 모뎀
🚱 접근성 센터	📖 키보드	🍟 폴더 옵션
🚾 프로그램 및 기능	🔣 홈 그룹	

2. 보안을 선택하고 바이러스 방지에 표시된 바이러스 백신 목록을 확인합니다.



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

	╢어판 항목 ▶ 관리 센터 🚽 😽 제어판 검색 🔎
제어판 홈 관리 센터 설정 변경	최근 메시지 검토 및 문제 해결 관리 센터에서 사용자의 확인이 필요한 문제를 하나 이상 발견했습니다.
사용자 계정 컨트롤 설정 변경 보관된 메시지 보기	보안(S) 🛞
성능 정보 보기	스파이웨어 및 원치 않는 소프트웨어 방지 (중요) 볼 Windows Defender의 상태가 최신이 아닙니다. 참고: 둘 이상의 바이러스 백신 프로그램을 동시에 실행하면 컴퓨터 실행이 느려질 수 있습니다. 스파이웨어 및 관련 보호에 대한 메시지 끄기 사용 가능한 옵션 보기
	바이러스 방지 (중요) AhnLab V3 Internet Security 8.0이(가) 꺼져 있습니다. 바이러스 방지에 대한 메시지 끄기 온라인으로 다른 바이러스 백신 프로그램 가져오기
	Windows Update Windows Update가 사용자 확인 후 업데이트를 다운로드하여 설치하도록 설정되 성 있습니다. Windows Update에 대한 메시지 끄기
	유지 관리(M)
	백업 설정 파일이 백업되고 있지 않습니다. Windows 백업에 대한 메시지 끄기
참고 항목 백업 및 복원 Windows Undete	해결하려는 문제를 찾을 수 없으면 다음 중 하나를 시도해 보십시오.
Windows opuate Windows 프로그램 호환성 문제 해결사	문제 해결(O) 문제 찾기 및 해결 북구(R) 문제 찾기 및 해결

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 여부와 바이러스 백신 실행 여부에
 대한 상세 결과를 나타냅니다.
 - 바이러스 백신 설치 여부: 설치 안 함으로 나타나면 백신 상태 확인하기를 눌러 관리 센터에 등록된 백신 정보가 있는지 확인합니다.
 - 바이러스 백신 실행 여부: 실행 안 함으로 나타나면 백신 상태 확인하기를 눌러 Windows 관리 센터에서 바이러스 백신이 사용 중으로 표시되는지 확인합니다.

점검 항목 상세 정보		
점검 결과: 취약	*	백신 상태 확인하기
바미러스 백신 설치 며부 - <mark>설치</mark> 바미러스 백신 실행 여부 - <mark>실행 안 함</mark> ▶ 설치된 바미러스 백신을 실행하십시오,		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍		
니다. ★바미러스 백신을 사용 중임에도 점검 결과가 '취약'으로 판정되는 경우, 조치 방법 상세 안내 > FAQ를 침 고하십시오.	ł	
	-	<u>조치 방법 상세 안내</u>

한참고

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

 바이러스 백신의 최신 보안 패치 여부: 업데이트 필요로 나타나면 관리 센터 실행하기를 눌러 보안 센터에 등록된 바이러스 백신이 최신 업데이트 상태인지 확인합니다.

점김 항복 상세 정모		
점검 결과: 취약	*	관리 센터 실행하기
바이러스 백신 설치 여부 - 설치 바이러스 백신 실행 여부 - 실행 바이러스 백신의 최신 보안 패치 여부 - 업데이트 필요 ▶ 설치된 바이러스 백신의 최신 보안 패치를 적용하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍		
* 바이러스 백신을 사용 중입에도 점검 결과가 '취약'으로 판정되는 경우, 조치 방법 상세 안내 > FAQ를 참		
	Ŧ	<u>조치 방법 상세 안내</u>

한참고

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

조치 방법

바이러스 백신 최신 업데이트 상태를 확인하는 방법은 다음과 같습니다.

Windows XP SP2 이상 버전

- Windows 작업 표시줄의 시작 > 설정 >제어판을 선택한 후 클래식 보기로 전환을 선택하여 보안 센터를 실행합니다.
- 2. 보안 센터에서 바이러스 백신을 선택하여 설치된 바이러스 백신을 확인합니다.
 - 바이러스 백신이 최신 엔진으로 업데이트된 상태가 아니라면 최신 버전 아님으로 표시됩니다.
 설치된 바이러스 백신의 업데이트를 실행합니다.
 - 바이러스 백신이 최신 엔진으로 업데이트된 상태라면 사용 중으로 표시됩니다.

한참고

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



Windows Vista

- Windows 작업 표시줄의 시작 > 설정 > 제어판을 선택한 후 클래식 보기로 전환을 선택하여 보안 센터를 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.



한참고

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 > 제어판에서 보기 기준을 작은 아이콘으로 전환하고 관리 센터를 선택합니다.

중 ♥ ♥ ♥ 제어판 ▶ 모든 제이	판 항목 ▶	 ◄ 제어판 검색
컴퓨터 설정 변경		보기 기준: 작은 아이콘 ▼
🎭 BitLocker 드라이브 암호화	✔ Flash Player(32비트)	🞒 ODBC(32비트)
🗃 Realtek HD 오디오 관리자	🐻 RemoteApp 및 데스크톱 연결	📑 Windows CardSpace
Windows Defender	Windows Update	🔗 Windows 방화벽
🖉 개인 설정	🔞 관리 도구	🏲 관리 센터
🔊 국가 및 언어	🚺 글꼴	😿 기본 프로그램
🔐 날짜 및 시간	🕎 네트워크 및 공유 센터	🔞 동기화 센터
🖳 디스플레이	⑦ 마우스	🥥 메일
🔳 문제 해결	📑 바탕 화면 가젯	🐌 백업 및 복원
🌮 복구	🎎 사용자 계정	📮 색 관리
🚨 색인 옵션	🔳 성능 정보 및 도구	📢 소리
1型 시스템	🎒 시작	🔜 알림 영역 아이콘
🍱 위치 및 기타 센서	🖶 음성 인식	🔂 인터넷 옵션
🛃 인텔® HD 그래픽	🙆 자격 증명 관리자	튫 자녀 보호
📑 자동 실행	🛄 작업 표시줄 및 시작 메뉴	🚇 장치 관리자
📾 장치 및 프린터	🗃 전원 옵션	📟 전화 및 모뎀
🚱 접근성 센터	⊇ 키보드	📓 폴더 옵션
👼 프로그램 및 기능	🔞 홈 그룹	

- 2. 보안을 선택하고 바이러스 방지에 표시된 바이러스 백신 목록을 확인합니다.
 - 바이러스 백신이 최신 업데이트 상태가 아닌 경우 최신 상태가 아닙니다. 라고 표시됩니다. 지금
 업데이트를 눌러 바이러스 백신의 업데이트를 실행합니다.


한참고

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.

• <u>안랩 V3 다운로드 사이트 바로가기</u>

한참고

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 안전으로 표시됩니다.
- 취약: 점검 결과가 취약으로 나오는 경우, PC 에 설치되지 않는 중요 업데이트가 존재하는 것으로
 나옵니다. 미설치 업데이트 보기를 눌러 설치되지 않은 중요 업데이트를 설치하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	미설치 업데이트 보기
PC에 1개의 설치되지 않은 중요 업데이트가 있습니다. ▶ [중요 업데이트 설치하기]를 눌러 모든 설치되지 않은 중요 업데이트를 설치하십시오.		
1. Microsoft 보안 공지: Windows 7 및 Windows Server 2008 R2에 대한 자격 증명 보호 및 관리를 개선 하는 업데이트: 2014년 9월 9일 (2982378)		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍		
	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

점검 결과가 **취약**일 때, <u>APM 라이선스가 없는 경우</u>와 <u>APM 라이선스가 있는 경우</u>에 따라 다음과 같이 조치하여 주시기 바랍니다.

[APM 라이선스가 없는 경우]

1. 미설치 업데이트 보기를 누릅니다.



2. <미설치 Windows 업데이트 목록>이 표시됩니다.

미설치 Windows 업데이트 목록 - 내PC지키미	×	
업데이트 이름	_	
Windows Server 2008 R2 x64 Edition용 업데이트(KB974431)	상세 정보 보기	
Windows Server 2008 R2 x64 Edition용 보안 업데이트(KB975467)	상세 정보 보기	
Windows Server 2008 R2 x64 Edition용 보안 업데이트(KB974571)	상세 정보 보기	
Windows Server 2008 R2 x64 Edition용 보안 업데이트(KB972270)	상세 정보 보기	
Windows Server 2008 R2 x64 Edition용 업데이트(KB977074)	상세 정보 보기 🚽	
· · · · · · · · · · · · · · · · · · ·		
입데이트 설명		
공격자가 사용자 몰래 시스템 작업이나 동작을 다르게 표시할 수 있는 보안 니다. Microsoft에서 제공하는 이 업데이트를 설치하며 시스템을 보호할 수 트를 설치한 후 시스템을 다시 시작해야 합니다.	문제가 확인되었습 있습니다. 이 업데이	
MS 업데이	트 사이트 바로가기	
	닫기	

한참고

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.

한참고

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

Windows XP

- 1. IE 실행 후 **도구 > Windows Update**를 선택하거나 <u>http://www.update.microsoft.com</u>로 접속합니다.
- 2. Microsoft Update를 선택하거나 새로운 기능! 옆에 있는 이동을 누르십시오.

한참고

이전에 Windows 및 MS office 제품에 대한 업데이트를 적용한 적이 있는 경우에는 아래 <u>사용자 지정</u> <u>설치</u>로 이동하십시오.

🥙 Microsoft Windows 업데이트 - Wi	ndows Internet Explorer		
🗿 🕢 👻 http://update.microsoft.co	m/windowsupdate/v6/default.aspx?ln=ko	💌 😽 🗙 🔽 Bing	P
파일(E) 편집(E) 보기(Y) 즐겨찾기(A)	도구(D 도움말(H)		
촱 즐겨찾기 🛛 🏡 🍘 추천 사이트 🗸 🔊 무	료 Hotmail 🔊 연결 사용자 정의 🗿 Get more	e Add-ons +	
🗞 Microsoft Windows 업데이트		<u>∆</u> • ⊠ - ⊒ ⊜ •	표이지(P)· 안전(S)· 도구(Q)· 😧·
		바른 연광 (0	한민국 홈페이지 - 컨세계
💐 Windows		Microsoft, cor	n에서 검색: [검색]
Windows Update			
Windows 제품군 Windows 마켓플레이스	Office 제품군 Microsoft Update		
Windows 업데이트 홈	화영합니다!		A DC H#
1 A A A A A A A A A A A A A A A A A A A	Windows Update		V ruii
8년 업데이트 내역 강토 승거장 업데이트 역동 서적 분경	로운 기능! Microsoft 업데이트 하십시오!		자동 업데이트를 사용하면 사용 자의 컴퓨터에 대한 새로운 보안 업데이트가 자동으로 검사되고 설 치됩니다.
월 8 년 8 월 문 과 대답 컴 퓨 도움말 및 지원 보기 Window	터 를 최신·상태로 유지 #5. 하드웨어 또는 장치에 업데이트가 필요한지 #	확인하십시오.	자동 업데이트 설정
관리자 옵션 사용	른 설치 중요 업데이트 다운로!	드(퀸쟝)	·

3. 환영합니다. 화면이 표시되면 지금 시작을 눌러 Microsoft Update를 진행합니다.

Microsoft Update – Microsoft Internet Explorer	
파얼(E) 편집(E) 보기(Y) 즐겨찾기(A) 도구(D) 도움망(U)	
🌀 সর • 🕥 · 🖹 📓 🏠 🔎 রধ 🦅 জ্ञসর্থস 🤣 🍰 🕫 • 🥃	劉 - 8
卒企(1) 函 http://www.update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx?returnurl=http:	://www.update,microsoft.com/mic 🗹 🔁 미동 연결 🇯
	빠른 연결 대한민국 홈페이지 전세계
Microsoft	Microsoft.com에서 검색: 검색
Microsoft Update	
환영합니다! Microsoft Update	
Microsoft Update를 지금 사용해 보세요.	
이제 Windows, Office 및 기타 Microsoft 응용 프로그램에 대한 로드할 수 있습니다. Microsoft Update는 Windows Update의 모 롯한 기타 Microsoft 응용 프로그램에 대한 다운로드를 제공하는 지글시작	업데이트를 모두 한 장소에서 다운 든 기능과 이점은 물론 Office를 비 새로운 서비스입니다. v

4. 계속을 누릅니다.

Microsoft Update – Microsoft Internet Explorer	
파얼(E) 편집(E) 보기(V) 즐겨찾기(A) 도구(I) 도움말(U)	A
🌀 सन्द्र 🔹 💿 📓 🚱 🔎 येथ् 🌟 इत्रव्रंग 🤣 🎯 🎭 😼 🦓	
주소(D) 🍓 http://www.update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx?returnurl=http://www.update 😪 🛃	이동 연결 »
타른 연결 대한민국 홈페이지 전세계	
Microsoft Microsoft Microsoft com에서 검색:	검색
Microsoft Update	
환영합니다! Microsoft Update	
라이센스 계약 검토 이 웹 사이트를 사용할 때는 사용자가 선택한 업데이트에 원래 Microsoft 제품의 라이센스 계 약이 적용될 수 있습니다. Microsoft 제품 중 일부 라이센스 계약에는 해당 제품에 대한 업데 이트에도 적용된다는 내용이 표시되어 있습니다.	
또한 제품 설치 중에 사용자가 적용 가능한 라이센스 계약 사본을 검토하지 않고 이후 업데이 트에 동의했을 수도 있습니다.	
为今	
<u>Microsoft Update 개인 정보 보호 정책</u> ©2008 Microsoft Corporation, All rights reserved. <u>사용약관 상표 개인정보보호</u> 법적정보	
2 인터넷	,d

5. IE 알림 표시줄에서 마우스 오른쪽을 눌러 ActiveX 컨트롤 설치를 누릅니다.

Microsoft Update - Microsoft Internet Explorer	
파알(E) 편집(E) 보기(Y) 즐겨찾기(A) 도구(I) 도움말(H)	<u></u>
🔇 नड • 🕥 · 💌 🖉 🐔 🔎 देव 🤺 छन्नेप्रंग 🤣 😥 🌭	
주소(①) (書) http://www.update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx?returnurl=http://v	www.update.microsoft.com/micros 🗸 🄁 01동 - 연결 🏾
🜍 이 사이트에서 'Microsoft Corporation'에서 배포한 'Microsoft Update' ActiveX 컨트롤을 필요로 합니다.	해당 ActiveX 컨트롤을 설치하려면 여기를 클릭하십시오, 🗙
	화는 연결 대한민국 올레이지 전세계 Microsoft com에 U 2001
Microsoft	Microsoft.com에서 음악: 검색
Microsoft Update	
환영합니다!	^
N Melosort opune	
웹 사이트를 표시하는 데 필요한 ActiveX 컨트롤을 설치합니다. 이 컨트롤이 없으면 컴퓨터에 웹 사이트가 제대로 표시되지 않습니다. 설치하려면 다음을 수향하십시오.	
1. Internet Explorer 알림 표시물을 마우스 오른쪽 단추로 클릭합니다. 알림 표시물은 주소 표시줄 바로 아곱 2. 마우스 오른쪽 단추 메뉴에서 ActiveX 컨트롤 설치를 클릭합니다. 3. 보안 경고 대화 상자에서 설치을 클릭합니다.	에 있습니다.
해: Internet Explorer 알림 표시줄의 마우스 오른쪽 단추 메뉴	
주会()) 合http://www.microsoft.com/downloads/search_aspx?displ	
今 이 사이트를 표시하려면 다음 ActiveX 컨트롤이 좋으합니다.	
ActiveX 范围基 监知(C)	
Microsoft	
EO #VE #DEW	*
<u>Microsoft Update 개인 정보 보호 정책</u> @2008 Microsoft Corporation, All rights reserved, <u>사용약관</u> <u>상표</u> <u>개인정보보호</u> <u>법적정보</u>	
9	🕐 인터넷

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

Internet	Explorer - 보안 경고 🛛 🔀
이 소프	트웨어를 설치하시겠습니까? 이름: <u>Microsoft Update</u> 게시자: <u>Microsoft Corporation</u>
※ 자사	예한 옵션 보기(<u>0</u>) 설치 안 함(<u>D</u>)
1	이 형식의 파일은 사용자의 컴퓨터에 피해를 줄 수 있습니다. 신뢰할 수 있는 게시 자로부터의 소프트웨머만 실행하십시오, <u>위험성</u>

자동 업데이트 설정이 되어 있지 않은 경우 아래 화면과 같이 자동 업데이트 사용 설정 화면이 나타납
 니다. 자동 업데이트 사용을 누릅니다.

Microsoft Update – Microsoft Internet Explorer	
파일(E) 편집(E) 보기(V) 즐겨찾기(A) 도구(I) 도움말(比)	an a
🔇 नड • 💭 · 🗷 🙆 🏠 🔎 छथ 👷 छत्र थेत्र। 🤣 😥 🦓 📰	
주소(D) 🚳 http://www.update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx?in=ko&muopt=1&	returnurl=http://www.update.micro 💌 🔂 미동 - 연결 🌣
	略은 연결 대한민국 홈페이지 전세계
Microsoft	Microsoft.com에서 검색: 검색
Microsoft Update	
환영합니다! Microsoft Update	^
자동 업데이트 설정을 변경하시겠습니까? Windows는 사용자가 지정한 일정에 따라 사용자 컴퓨터 및 프로그램에 가장 중요한 업데이트를 자동으로 할 수 있습니다. 컴퓨터를 최신 강태로 유지할 수 있는 가장 쉽고 빠른 방법입니다.	益丸
자동 업데이트: 사용 안 함 <u>자동 업데이트 사용</u> 중요 업데이트가 제공될 때 이를 자동으로 신치되지 않습니다. 중요 업데이트를 모두 설치하기 견에는 컴퓨터가 안전하지 않을 수 있습니다.	
업데이트 확인	
<u>Microsoft Update 개인 정보 보호 정책</u> @2008 Microsoft Corporation, All rights reserved, <u>사용약관</u> <u>상표</u> <u>개인정보보호</u> <u>발적정보</u>	
8)	👛 인터넷

 <자동 업데이트>가 나타나면 새 업데이트 설치에서 매일로 설정합니다. 매일로 시간을 설정하면 설정 된 시간에 자동 업데이트가 수행됩니다.

👋 자동 업데이트 🛛 💈
자동 업데이트를 사용하면 사용자 컴퓨터를 안전하게 보 호합니다.
자동 업데이트를 사용하면 Windows에서 주기적으로 최신 업데이트를 확인하고 사용자 컴퓨터에 자동으로 설치합니다. 보안 업데이트, 중요한 업데이트, 서비스 팩 등과 같은 업데이트를 설치합니다. <u>자동 업데이트를 사용해야 하는 이유</u> 새 업데이트 설치: 매일 ✔ 시 오전 3:00 ✔
사용자에 대한 어떠한 정보도 수집하지 않습니다. <u>Windows Update 개인 정보 보호 정책</u> 을 읽으십시오.
확인 기타 옵션(N) 나중에 설치(L)

사용자 지정 설치

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

 IE 실행 후 도구 > Windows Update를 선택하거나 <u>http://www.update.microsoft.com</u>로 접속한 후 사용자 지정 설치를 누릅니다.



2. 업데이트 목록이 나타나면 업데이트 검토 및 설치를 눌러 설치를 시작합니다.

한참고

해당 업데이트에 대한 자세한 정보를 확인하려면 해당 업데이트를 누르면 정보가 표시됩니다. 설치하지 않을 항목에 대해서는 <u>업데이트 숨기기</u>를 설정하면 점검 대상에서 제외됩니다.

🖉 Microsoft Windows 업데이	🗏 – Windows Internet Explorer	
🕘 🗢 💊 http://update.mi	crosoft,com/windowsupdate/v6/default,aspx?in=ko	💌 🍫 🗙 🔁 Bing
파일(E) 편집(<u>E</u>) 보기(⊻) 클기	계찾기(<u>A</u>) 도구(<u>T</u>) 도움말(<u>H</u>)	
👷 즐겨찾기 🛛 🍰 🏉 추천 사이트	🕞 🖉 무료 Hotmail 🔊 연결 사용자 정의 🍃 Get more Add	l-ons •
🍓 Microsoft Windows 업데이트		🙆 • 📾 - 🗆 🖨
		빠른 연결
💐 Windows		Microsoft.
Windows Update		
Windows 제품군 Windows 마켓	플레이스 Office 제품군 Microsoft Update	
Windows 업데이트 홈	📣 검색 결과 사용자 지정	
🛐 업데이트 설치 (80)	중요 업데이트 선택 보안 위협 및 성능 문제로부터 컴퓨터를 보호하기 위해 중요 입	데이트를 모두 설치하는 것이 좋습니
종류별 선택		
중요 업데이트 (80)	🔁 `앱데이트 검토 및 절치	
소프트웨어, 선택적 (11) 하드웨어, 선택적 (1)	중요 업데이트 모두 지우기 모두 선택	
옵션	Microsoft Windows XP	
업데이트 내역 검토	♥ Windows XP용 보안 업데이트(KB2807986)	
숨겨진 업데이트 복원 설정 변경	VI Windows XP용 Internet Explorer 8 누적 보안 업	데이트(KB2809289)
질문과 대답	♥ Windows 악성 소프트웨어 제거 도구 - 2013년 3월	(KB890830)
도움말 및 지원 보기	♥● Windows XP용 보안 업데이트(KB2778344)	

3. 업데이트 설치를 누릅니다.

🌈 Microsoft Windows 업데이	⊑ - Windows Internet Explorer	
🕘 🗢 💊 http://update.mid	rosoft,com/windowsupdate/v6/default,aspx?in=ko	🖌 🛃 🔀 Bing
파일(E) 편집(<u>E</u>) 보기(⊻) 즐겨	찾기(<u>A</u>) 도구(<u>I</u>) 도움말(<u>H</u>)	
🚖 즐겨찾기 🛛 🚖 🏉 추천 사이트	• 🔊 무료 Hotmail 🔊 연결 사용자 정의 🍃 Get more Add-ons	•
🌯 Microsoft Windows 업데이트		🙆 • 🗟 • 🗆 🖷
		빠른 연결
💐 Windows		Microsof
Windows Update		
Windows 제품군 Windows 마켓링	플레이스 Office 제품군 Microsoft Update	
Windows 업데이트 홈	📣 검색 결과 사용자 지정	
▶ 업데이트 설치 (80)	업데이트 검토 및 설치	
종 류별 선택 중요 업데이트 (80)	[집데이트 결치] 현재 연결 속도에서의 예상 시간: 48 분	
소프트웨어, 선택적 (11)	중요 업데이트	
하드웨어, 선택적 (1)	Microsoft Windows XP	
84	♥ ♥ Windows XP용 보안 업데이트(KB2807986)	
업데이트 내역 검토	♥ Windows XP용 Internet Explorer 8 누적 보안 업데이트	(KB2809289)
숨겨진 업데이트 복원	♥ Windows 약성 소프트웨어 제거 도구 - 2013년 3월(KB89	0830)
설정 변경		
질문과 대답		
도움말 및 지원 보기	☑ Windows XP용 보안 업데이트(KB2799494)	

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

😵 업데이트 설치 🛛 🔀
👌 업데이트를 다운로드하고 설치하는 중
설치 상태:
Windows XP SP3용 Windows Media 형식 런타임 9, 9,5 및 11 보안 업데이트 (KB978695) 다운로드 조중(업데이트 1 / 80) 중(업데이트 1 / 80)
다운로드 중:
취소

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 Update를 선택합니다.

한참고

이전에 Windows 및 MS office 제품에 대한 업데이트를 적용한 적이 있는 경우에는 아래 <u>업데이트 설치</u>로 이동하십시오.

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

<> < < < < < < < < < < <	Windows Update	▼	٩
↔ 업데이트 확인 설정 변경	Windows Ultimate Extras	를 사용한 Windows Up	Ø date
업데이트 기록 보기	🛞 컴퓨터에 대한 업데이	트 확인	
숨겨진 업데이트 복원 ② 업데이트: 질문과 대답	컴퓨터의 보안 및 성능을 개신 이트를 설치하십시오.	1하려면 항상 최신 업데 🧮	겁데이트를 확인합니다(C).
射 Windows Ultimate Extras에 대 해 알아보기			
애 할아오기 참고 항목 보안 센터 설치된 업데이트	최근 업데이트 확인: 없음 설치된 업데이트: 없음 업데이트 설정: 업데이트를 특 받을 업데이트: Windows만	밖인하지 않음(권장하지 않음) 등에 대한 업데이트 얻기	

IE가 실행되면 사용 약관에 동의함을 선택하고 설치를 눌러 Microsoft Update를 사용하도록 설정합니다.

CO V Intp://update.microsoft.com/microsoftupdate/v6/vistadefault.aspx?ln=ko
😭 🍄 🌈 Microsoft Update
Nindows [.]
Microsoft Update
Windows, Office 등의 업데이트 다 운로드 Microsoft Update를 사용하면 Windows Update에서 제공하는 것과 동일한 중요 및 권장 Windows 업데이트뿐 마니라 Office와 다른 Microsoft 프로그램에 대한 다운로드도 받을 수 있습니다. 이 서비스는 컴퓨터를 보호하고 최신 상태로 유지시켜 주는 무료 서비스입 니다.
Windows Update 열정을 사용하며 사용으로 데미트를 세용하고 열차하다, 열차율 업데이트를 직접 선택할 수 있습니다. 시작하려면 Microsoft Update 소프트웨어를 설치 하십시오. 중요 및 권장 업데이트를 사용할 수 있을 때 컴퓨터에서 해당 업데이트를 받을 수 있도록 Windows 자동 업데이트가 기본적으로 설정됩니다.
MICROSOFT UPDATE 사용권에 대한 고지 사항 Microsoft Update 사용은 사용권에 대한 고지 사항의 적용을 받습니다. 동의하지 않는 경 우 Microsoft Update를 사용하지 못할 수도 있습니다. Microsoft Update의 각 페이지 하 단에 있는 링크를 통해 언제든지 내용을 검토할 수 있습니다.
 ✓ 사용 약관에 동의함 ☞ 설치
<u>Microsoft Update 개인 정보 보호 정책</u> @2008 Microsoft Corporation, All rights reserved, <u>사용약관</u> <u>상표</u> <u>개인정보보호</u> <u>법적정보</u>

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



업데이트 설치

- 1. 작업 표시줄의 **시작 > 모든 프로그램**에서 Windows Update를 선택합니다.
- 2. 제어판의 Windows Update가 나타나면 업데이트 설치를 누릅니다.



한참고

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 프로그램에서 Windows Update를 선택합니다.



2. Windows와 MS Office에 대한 최신 업데이트를 설치하려면 추가 정보 얻기를 선택합니다.



 IE가 실행되면 Microsoft Update 사용권에 대한 고지 사항에 동의합니다 를 선택하고 설치를 눌러 Microsoft Update를 실행합니다.

Alicrosoft Update - Windows Internet Explorer
thtp://www.update.microsoft.com/microsoftupdate/v6/vistadefault.aspx?ln=ko
☆ 즐겨찾기
Nindows [.]
Microsoft Update
Windows, Office 등의 업데이트 다 운로드 Microsoft Update는 컴퓨터를 보호하고 최신 상태로 유지시켜 주는 무료 서비스입니다. 이 서비스는 Windows, Office 및 다른 Microsoft 소프트웨어에 대한 업데이트를 제공할 뿐 아니라 새로운 Microsoft 소프트웨어도 옵션으로 제공합니다. 새 옵션 소프트웨어는 자동으로 설치되지 않습니다.
Vicrosoft Opdate 사용권에 대한 묘지 사항에 공격합니다;
<u>Microsoft Update 개인 정보 보호 정책</u> ©2010 Microsoft Corporation, All rights reserved, <u>사용약관</u> <u>상표</u> <u>개인정보보호</u> <u>법적정보</u>

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

🏉 Microsoft Upda	ate - Windows Internet Explore	er		X
G 🔾 🗸 🙋	http://www.u 👻 🚱	🗙 🚼 Google		+ م
🚖 즐겨찾기	🏉 Microsoft Update	📄 🏠 🔻 🗟 👻 🖃 🖷	9 ▼ 페이지(<u>P</u>) ▼	**
		- 빠른 연결 대한민국 홈페이)	지 전세계	
🛛 🍠 Win	dows [.]	Microsoft,com베셔 검색:		검색
Microsoft I	Update			
업데이트	를 확인하려면 시	니작 메뉴를 선택히	+십시오.	
Micros	soft Update를 성공적으로	설치했습니다.		
Windows Updat Windows Updat	e는 제어판에 포함되어 있습니 e가 자동으로 표시되지 않는 경	다. 업데이트를 확인하려고 하거 경우:	나 웹 페이지에	Ш
🍬 시작, 모든 프	프 로그램 을 차례로 클릭한 다음	음 Windows Update를 클릭합니[_ }.	
▶ 모든 프로 <i>프로그램 및</i>	그램 파일 검색 오	 Windows Update 보조프로그램 1 뒤로 프로그램 및 파일 검색 5 		
Microsoft Update	e <u>개인 정보 보호 정책</u> Corporation, All rights reserv	ved 사용약과 산표 개이제1	ㅋㅂㅎ	
법적정보				soft
	😻 인터넷 모오 -	모드: 설정	· · · · · · · · · · · · · · · · · · ·	• •

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.

점김 항목 상세 정보		
점김 결과: 취약	^	미설치 업데이트 보기
PC에 1개의 설치되지 않은 중요 업데이트가 있습니다. ▶ [중요 업데이트 설치하기]를 눌러 모든 설치되지 않은 중요 업데이트를 설치하십시오.		
1, Microsoft 보안 공지: Windows 7 및 Windows Server 2008 R2에 대한 자격 증명 보호 및 관리를 개선 하는 업데이트: 2014년 9월 9일 (2982378)		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍		
	Ŧ	<u>조치 방법 상세 안내</u>

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

🔀 패치 정보 보기 - AhnLab Pa	tch Management		
적용되지 않은 최신 모두 보기 💽	!패치가 6개있습니다.	지금 적용하시겠습니까? ▶ <u>적용된 패</u>	치목록 💽
□ □ 패치 분류 □ 위험!	도 패치번호 피	배치이름	패치 발표일
8 · · · · · · · · · · · · · · · · · · ·	긴급 MS15-011 그	L륨 정책의 취약성으로 인한 원격 코드 실행	2015/02/10
운영 체제 패치	중요 MS-KB3004 W	/indows 명령줄 감사용 업데이트 (3004375)	2015/02/10
운영 체제 패치 💷	- 중요 MS15-014 그	L룹 정책의 취약성으로 인한 보안 기능 우회	2015/02/10
운영 체제 패치 💷	- 중요 MS15-015 Mi	icrosoft Windows의 취약성으로 인한 권한	2015/02/10
운영 체제 패치 💷	중요 MS-KB3021 W	/indows 7 SP1 성능 개선을 위한 업데이트 (2015/02/15
운영 체제 패치 🛄	중요 MS-KB2731 W	/indows 7 또는 Windows Server 현지 시간	2012/10/08
		지금 업데이트	취소

3. 지금 업데이트를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.

4. 패치 적용이 완료되면 화면 상단의 적용된 패치 목록을 눌러 설치된 패치 정보를 확인할 수 있습니다.

역용된 패치 목록 - /	AhnLa	b Patc	h Management	THE R. LEWIS		X
총 206 개						
패치 분류	위험	님도	패치 번호	패치 이름	패치 발표일	
운영 체제 패치		긴급	MS15-011	그룹 정책의 취약성으로 인한 원격 코드 실행	2015/02/10	
운영 체제 패치		중요	MS-KB3004	Windows 명령줄 감사용 업데이트 (3004375)	2015/02/10	
운영 체제 패치		중요	MS15-014	그룹 정책의 취약성으로 인한 보안 기능 우회	2015/02/10	
운영 체제 패치		중요	MS15-015	Microsoft Windows의 취약성으로 인한 권한	2015/02/10	
운영 체제 패치		중요	MS-KB3021	Windows 7 SP1 성능 개선을 위한 업데이트 (2015/02/15	
운영 체제 패치		중요	MS-KB2731	Windows 7 또는 Windows Server 현지 시간	2012/10/08	
운영 체제 패치		긴급	MS15-020	Microsoft Windows의 취약성으로 인한 원격	2015/03/10	
운영 체제 패치		긴급	MS15-018	Internet Explorer용 누적 보안 업데이트(303	2015/03/10	
운영 체제 패치		긴급	MS15-021	Adobe 글꼴 드라이버의 취약성으로 인한 원	2015/03/10	
오피스 패치		중요	MS15-022	Microsoft Office의 취약성으로 인한 원격 코드	2015/03/10	
운영 체제 패치		중요	MS15-023	커널 모드 드라이버의 취약점으로 인한 권한	2015/03/10	
운영 체제 패치		중요	MS15-024	PNG 처리의 취약점으로 인한 정보 유출 문제(2015/03/10	
운영 체제 패치		중요	MS15-025	Windows 커널의 취약점으로 인한 권한 상승	2015/03/10	
운영 체제 패치		중요	MS15-028	Windows 작업 스케줄러 취약점으로 인한 보	2015/03/10	
운영 체제 패치		중요	MS15-029	Windows 사진 티코터 구성 요소의 취약점으	2015/03/10	
운영 체제 패치		중요	MS15-031	Schannel의 취약성으로 인한 보안 기능 우회	2015/03/10	
운영 체제 패치		중요	MS15-030	원격 데스크톱 프로토콜의 취약점으로 인한	2015/03/10	-
L						÷.
					취소	

한참고

자동 패치 시스템을 이용하는 경우 점검 결과가 PC 의 실제 보안 상태와 다르게 나타날 수 있습니다. 보안 정책에 따라 설치하지 않는 업데이트는 <mark>업데이트 숨기기</mark>를 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 설치하기를 눌러 최신 보안 업데이트를 설치하십시오.

점검 항목 상세 정보



한 한 고

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, <u>APM 라이선스가 없는 경우</u>와 <u>APM 라이선스가 있는 경우</u>에 따라 다음과 같이 조치하여 주시기 바랍니다.

[APM 라이선스가 없는 경우]

한글 2002 버전

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

AhnLab 내 PC 지키미 에이전트 사용설명서

				Ξ Ξ Σ
+ 🕘 🥖 http://www.hanco	om.com/ ♀ ♂ ₹	· 글로벌 소프트웨어 리더, ×		6 🛠 🖗
파일(F) 편집(E) 보기(V) 즐	'겨찾기(A) 도구(T) 도움	:말(H)		
_				
			로그인 회원가입 마이페이지 뉴스	5/이벤트 ENGLISH
hinron 2	회사소개 시	ነ업/제품 PR/IR 인재채용 고객센터	쇼핑몰 】문서서식센터 】 씽크프리	넷피스 24
한글과컴퓨터	FAQ Q&A 제품	품등록/인증 다운로드 기술지원 파트너 프로그램 구매지	원 교육지원	
•				
- / 7월 / 서태 / 도리				
고/객/엔/터				
FAQ		h 자료실		
Q& A				
제 품등록/인 증	LIGE			
	ΠαΓ			
421_ P	재미, 정보	¹ , 혜택까지 모두 받아가는 H&Friends 지금 바로, 함께하실		V T 🚫
뉴어				
체험판		제품명 전제전택 🗸 💿 세목 🔾 내용	검색 결과 내 검색	
패치 업데이트	비효	계모	지 정 비 이 드 근 일	
제품별 매뉴얼	<u> </u>			<u>, uz</u>
HWP 파일포맷	39 H	WP 파일 Form&1의 승개 해키오피스 2014 개최과 관련 제비 제고	2014-04	-00 /
기타 자료실	30 12	!쉽도피는 2014 세법엔 전년 영보 세종	2013-10	-01 15
기술지원	3/ 2	[김조피수 사중 업데이트 패시 파일 나운도는 안내 기능과]] 차락유피스 2014 \전 어머리트 파일 (차) 구 01 0 2229	E) 2012-10	-10 136407
파티네 파리그램	36 [.	기중패지] 안감도피스 2014 VP 쉽데이트 파일 (한/ 볼 9,1,0,2338	s) 📙 2015-03	-51 /954
파트너 프로그램	35 [.	기둥패지] 한김오피스 한/글 2014 VP 입네이트 파일 (한/글 9.1.0	1, 2338) 📙 2015-03	-31 3383

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.

한참고

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.

점검 항목 상세 정보		
점경 결과: 취약 PC에 성치되 하국 2014 (9102522)에 대한 치시 보안 언데이트를 성치해야 한다.	*	업데이트 설치하기
 ▶ [업데이트 설치하기]를 눌러 최신 보안 업데이트를 설치하십시오. 		<u>한컴 홈페이지</u>
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
* 한컴 자동 업데이트 프로그램에서 최신 버젼으로 표시되고 있으나 점겸 결과가 '취약'으로 판정되는 경 우, 한컴 홈페이지에서 최신 업데이트를 직접 다운로드하며 설치하십시오.		
		<u>조치 방법 상세 안내</u>
	4	

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

모두	보기 💌 1개	년 선택			· <u>적용된 패치 목록</u>	,
	패치 분류	위험	성도	패치 변호	패치 이름	I
	일반 SW 패치	1111	긴급	MS15-057	Windows Media Player의 취약성으로 인한 원격 코드 실행 문	2
	일반 SW 패치		긴급	MS12-016	.NET Framework 및 Microsoft Silverlight의 취약점으로 인한	2
	일반 SW 패치		긴급	MS12-025	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (2
	일반 SW 패치	00	긴급	MS12-035	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (2
	일반 SW 패치		긴급	M512-038	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (2
	일반 SW 패치		긴급	MS12-045	Microsoft Data Access Components의 취약점으로 인한 원격	-
~	일반 SW 패치	-	긴급	HNC 2010	HNC 2010 업데이트 (000858)	1
	일반 SW 패치	1111	긴급	MS-KB2820331	Windows 7 및 Windows Server 2008 r 2에 대 한 응용 프로	2
	일반 SW 패치	1111	긴급	MS-KB2786081	로그 오프하거나 Windows 7 SP1 또는 Windows Server 200	2
	일반 SW 패치		긴급	MS-KB2552343	Windows 7 또는 Windows Server 2008 R2가 실행되는 컴퓨	1
	일반 SW 패치	1111	긴급	MS-KB2813430	An update is available that enables administrators to update	1
	일반 SW 패치		긴급	MS13-053	Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드	-
	일반 SW 패치		긴급	MS13-057	Windows Media Format Runtime의 취약점으로 인한 원격 코	1
	일반 SW 패치	m	중요	MS13-058	Windows Defender의 취약점으로 인한 권한 상승 문제점 (28	2
	일반 SW 패치		긴급	Adobe Flash Player 14	Security updates available for Adobe Flash Player(APSB14-18)	-

3. 지금 업데이트를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.

4. 패치 적용이 완료되면 화면 상단의 적용된 패치 목록을 눌러 설치된 패치 정보를 확인할 수 있습니다.

H치 분류	위형	먹도	패치 변호	패치 이름	패치 발표일	패치 설치 날짜
2영 체제 패치		중요	MS15-060	Microsoft 공용 컨트롤의 취약성으로 인한 원격	2015/06/09	
2영 체제 패치	1111	긴급	MS15-067	RDP의 취약성으로 인한 원격 코드 실행 문제(3	2015/07/14	
발반 SW 패치		중요	Adobe	Adobe AIR Update (22.0.0.153)	2016/06/16	2016/06/21
반 SW 패치	1111	긴급	HNC 2010	HNC 2010 업데이트 (000858)	2016/04/19	2016/06/21
일반 SW 패치	1111	긴급	Adobe	Security updates for Adobe Reader and Acrob	2015/10/13	2016/06/21
방반 SW 패치	1111	긴급	MS-KB2	Windows 7 SP1, Windows Server 2008 R2 SP	2013/06/03	
운영 체제 패치		긴급	MS-KB2	Microsoft 보안 공지: 원격 데스크톱 프로토콜	2013/08/13	
응영 체제 패치		긴급	MS13-083	Windows 공용 컨트롤 라이브러리의 취약점으	2013/10/09	
발반 SW 패치	ш	중요	JAVA S	JAVA SE Runtime Environment 8 (008092)	2016/04/20	2016/06/21
2영 체제 패치	m	중요	MS-KB2	Windows 7 또는 Windows Server 현지 시간과	2012/10/08	
2영 체제 패치		중요	MS15-030	원격 데스크톱 프로토콜의 취약점으로 인한 서	2015/03/10	

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 않음으로 나타납니다. 패스워드 설정하기를 눌러 패스워드를 재 설정하거나 시작 > 제어판 > 사용자 계정을 선택하고, Windows 로그온 패스워드를 설정합니다.

점겸 항목 상세 정보		
점검 결과: 취약 로그온 패스워드 사용 - <mark>사용하지 않음</mark> ▶ [패스워드 설정하기]를 눌러 다음 항목을 준수하며 패스워드를 설정하십시오. 로그온 패스워드 설정 규칙에 따라 다음과 같이 패스워드를 설정합니다. - 9자 이상	*	패스워드 설정하기
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

 로그온 패스워드가 사용자 계정과 동일한 것으로 나옵니다. 패스워드 설정하기를 누르거나 시작 > 제어판 > 사용자 계정을 선택하고, 사용자 계정에 사용된 문자열과 동일하지 않은 로그온 패스워드를 설정합니다.

점검 항목 상세 정보		
점검 결과: 취약 로그온 패스워드가 사용자 계정(●●)과(와) 동일합니다. ● [패스워드 설정하기]를 불러 다음 항목을 준수하여 패스워드를 설정하십시오. 로그온 패스워드 설정 규칙에 따라 다음과 같이 패스워드를 설정합니다. - 9자 미상 로그온 패스워드가 사용자 계정과 동일한지 점검합니다. * 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍니다.	*	패스워드 설정하기
	Ŧ	<u>조치 방법 상세 안내</u>

 로그온 패스워드의 길이 또는 필수문자 조합이 안전 조건을 준수하지 않는 것으로 나타납니다.
 패스워드 설정하기를 누르거나 시작 > 제어판 > 사용자 계정을 선택하고, 패스워드의 길이와 필수문자 조합이 안전 조건을 준수하도록 패스워드를 설정합니다.



 로그온 패스워드를 점검하지 않고, 패스워드 검사 건너뛰기를 한 경우입니다. 패스워드 입력하기를 누르거나 시작 > 제어판 > 사용자 계정을 선택하고 Windows 로그온 패스워드를 다음의 안전 조건을 준수하여 설정합니다.

점검 항목 상세 정보		
점검 결과: 취약 사용자가 [패스워드 검사 건너뛰기]를 선택하여 점검이 볼가능합니다. ▶[패스워드 입력하기]를 눌러 로그온 패스워드의 안전성 여부를 점검하십시오. 안전하지 않은 경우, 다 음 항목을 준수하며 로그온 패스워드를 설정하십시오. 로그온 패스워드 설정 규칙에 따라 다음과 같이 패스워드를 설정합니다. - 9자 이상 * 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.	*	패스워드 입력하기
	Ŧ	<u>조치 방법 상세 안내</u>

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.

로그인 패스워드 설정 - AhnLab 내PC지키미	4
PC의 로그인 패스워드를 설정합니다.	
로그인 패스워드 설정 규칙 1. 로그인 패스워드 설정 규칙에 - 9자 미상 2. 많이 사용하는 단머(사전 문지 3. 반복되는 문자열을 사용하지	따라 다음과 같이 패스워드를 설정합니다. 아)를 패스워드로 설정하지 않습니다. 않습니다.
현재 패스워드와 새 패스워드/새 패스	워드 확인을 입력하고 확인을 누르십시오.
현재 패스워드 새 패스워드 새 패스워드 확인	
	확인 취소

조치 방법

Windows 로그온 패스워드 설정 방법은 다음과 같습니다.

한참고

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 > 제어판을 선택한 후 제어판이 나타나면 클래식 보기로 전환합니다.
- 2. 사용자 계정을 선택합니다.
- 3. 사용자 계정 목록에서 패스워드를 변경할 계정을 선택합니다.

🏙 사용자 계정	
③ 뒤로 🕥 👷 홈	
참고	👷 사용자 계정
 2 사용자 계정 2 사용자 계정 유형 2 사용자 전환 	작업 선택
	▶ 계정 변경
	➡ 세 계정 만들기
	▶ 사용자 로그온 또는 로그오프 방법 변경
	또는 변경할 계정 선택
	ymuser 컴퓨터 관리자 암호 사용 전류터 관리자
	Guest 계정 사용 만 합

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

魐 사용자 계정	
Ġ 뒤로 📀 戅 홈	
<mark>관련 작업</mark> 다른 계정 변경 새 계정 만들기	ahnlab 계정의 어떤 정보를 변경하시겠습니까? 2 이름 변경 2 암호 만들기 2 그림 변경 2 계정 유형 변경 3 계정 삭제

• 기존 패스워드가 있는 경우: 암호 변경을 선택합니다.

😕 사용자 계정	
Ġ 뒤로 📀 👥 홈	
관련 작업 다른 계정 변경 새 계정 만들기	ahnlab 계정의 어떤 정보를 변경하시겠습니까?
	∋ 계정 삭제

Windows Vista

- 1. 시작 > 설정 > 제어판을 선택한 후 제어판이 나타나면 클래식 보기로 전환합니다.
- 2. 사용자 계정을 선택합니다.
- 3. 패스워드가 없는 경우 다음 화면에서 **사용자 계정에 대한 암호를 만듭니다**를 선택합니다.

ⓒ ♥ ♥ ▶ 제어판 ▶ 사용자	•계정 및 가족 보호 ▶ 사용자 계정	 ◆ → →	م
작업 암호 재설정 디스크 만들기	사용자 계정 변경		0
네트워크 암호 관리 파일 암호화 인증서 관리 고급 사용자 프로필 속성 구성 환경 변수 변경	사용자 계정에 대한 암호를 만듭니다. 사진 변경 중 계정 이를 변경 중 계정 유형 변경		est Idministrator
같이 단구 같이 참고 항목 중 자녀 보호	 ● 다른 계정 관리 ● 사용자 계정 컨트롤 사용/사용 안 함 		

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.

			- O - X
중 _ ♥ ♥ ▶ 제어판 ▶ 모든 제여	계판 항목 🕨	▼ 🍫 제어판 검색	Q
컴퓨터 설정 변경		보기 기준: 작은 아이콘 🔻	3
			-
The Bittocker 드다이브 암호화	RemoteApp 및 데스크톱 연결	Windows CardSpace	
Windows Defender	🖉 Windows Update	🔗 Windows 방화벽	=
🎑 개인 설정	泡 관리 도구	🏲 관리 센터	
🔊 국가 및 언어	. 글꼴	♂ 기본 프로그램	
📸 날짜 및 시간	👯 네트워크 및 공유 센터	🔞 동기화 센터	
💹 디스플레이	♂ 마우스	🥥 메일	
💽 문제 해결	📑 바탕 화면 가젯	🐌 백업 및 복원	
🗳 복구	👪 사용자 계정	📮 색 관리	
🚨 색인 옵션	📕 성능 정보 및 도구	패 소리	
A100			

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

10. 10 A.A.A	P 21.21		• X
중 < 20 < 20 < 20 < 20 < 20 < 20 < 20 < 2	제어판 항목 🕨 사용자 계정	▼ ⁴ → 제어판 검색	٩
제어판 홈 자격 증명 관리 암호 재설정 디스크 만들기 온라인 ID 연결 파일 암호화 인증서 관리 고급 사용자 프로필 속성 구성 환경 변수 변경	사용자 계정 변경 사용자 계정에 대한 암호를 만들니다. 사진 변경 ☞ 계정 이름 변경 ☞ 계정 유형 변경 ☞ 다른 계정 관리 ☞ 사용자 계정 컨트롤 설정 변경	ahnlab Administrator	2
😽 자녀 보호			

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

22-2-22			x
🚱 ◯ ♥ 💐 제어판 ▶ 모든 :	제어판 항목 🕨 사용자 계정	▼ 49 제어판 검색	٩
제어판 홈	사용자 계정 변경		0
자격 증명 관리 암호 재설정 디스크 만들기 온라인 ID 연결 파일 암호화 인증서 관리 고급 사용자 프로필 속성 구성 환경 변수 변경	암호 변경 암호 제거 사진 변경 양 계정 이름 변경 양 계정 유형 변경	ahnlab Administrator 암호 사용	
참고 항목 😵 자녀 보호	😵 다른 계정 관리 😵 사용자 계정 컨트롤 설정 변경		

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 설정하기를 누르거나 시작
 > 제어판 > 사용자 계정을 선택하고, Windows 로그온 패스워드를 설정합니다.

점검 항목 상세 정보		
점겸 결과: 취약	^	패스워드 설정하기
PC에 패스워드를 변경한 이후로 92 일이 지났습니다. ▶ 패스워드의 안전성을 유지하기 위해 <mark>90</mark> 일 이내로 패스워드를 변경하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
		<u>조치 방법 상세 안내</u>
	Ŧ	

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.

PC의 로그?	빈 패스워드를 설정합니다	ŀ.		
로그인	패스워드 설정 규칙			
1, 로그	1인 패스워드 설정 규칙에 미사	ㅔ 따라 다음과 같이 패스워드	를 설정합니다.	
2, 많0 3, 반복	이용하는 단어(사전 문 특되는 문자열을 사용하지	자)를 패스워드로 설정하지 (않습니다.	않습니다.	
현재 패스워	드와 새 패스워드/새 패스	스워드 확인을 입력하고 확인	을 누르십시오.	
	현재 패스워드			
	새 패스워드			
	새 패스워드 확인			
		🔲 패스워드 표시하기		
			±101	치스

한참고

Windows 의 패스워드 변경 기능을 직접 실행하려면 <u>로그온 패스워드 안전성 점검</u>을 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 조치를 눌러 화면 보호기를 설정합니다.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
화면 보호기의 <mark>암호가 설정되어 있지 않습니다.</mark> ▶ [화면 보호기 설정하기]를 눌러 화면 보호기의 암호를 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	~	<u>조치 방법 상세 안내</u>

 화면 보호기 대기 시간이 관리자가 지정한 시간 이상인 경우: 원클릭 조치를 눌러 대기 시간을 관리자가 지정한 설정 값으로 설정합니다.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
화면 보호기의 대기 시간이 10분을 초과하며 설정되어 있습니다.(현재 대기 시간 : 20분) ▶ [화면 보호기 설정하기]를 눌러 화면 보호기의 대기 시간을 10분 이하로 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

 화면 보호기의 비밀번호가 설정되어 있지 않은 경우: 원클릭 조치를 눌러 제어판의 화면 보호기 설정 화면에서 다시 시작할 때 암호로 보호를 선택합니다.

점김 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
화면 보호기의 <mark>암호가 설정되어 있지 않습니다.</mark> ▶ [화면 보호기 설정하기]를 눌러 화면 보호기의 암호를 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
		조치 방법 상세 안내
	Ŧ	

조치 방법

Windows XP

- 1. 시작 > 제어판에서 디스플레이를 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 보호를 선택합니다.

테마 바탕 화면 화면 5	보호기 화면 배색 설정
	-0
화면 보호기(<u>S</u>)	
3차원 곡선	M 설정(I) 미리 보기(Y)
3차원 곡선 대기(<u>₩</u>): 10 🗢 분	월 월청(Ţ) 미리 보기(⊻) 로 ♥다시 시작할 때 암호로 보호(₽)
3차원 곡선 대기(ឃ): 10 🗢 8 모니터 전원 모니터 전원	실정(Ţ) 미리 보기(♡) 로 ♥ 다시 시작할 때 암호로 보호(₽) 터 전원 설정을 조정하고 에너지를 절약하려면 [전 을 클릭하십시오. 전원(Q)

4. **확인**을 누릅니다.

Windows Vista / Windows 7

1. 바탕 화면에서 마우스 오른쪽을 누르고 개인 설정을 선택합니다.

V	새 폴더	
	보기(V)	•
	정렬 기준(O)	•
	새로 고침(E)	
	붙여넣기(A)	
	바로 가기 붙여넣기(S)	
	삭제 취소(U)	Ctrl+Z
	그래픽 속성	
	그래픽 옵션	•
2	SVN Checkout	
-	TortoiseSVN	•
	다음 바탕 화면 배경(N)	
	새로 만들기(W)	+
<u> </u>	화면 해상도(U)	
	가젯(G)	
2	개인 설정(E)	

- ◯ 🜍 ♥ 🖉 → 제어판 → 모든 제어판 항목 → 개인 설정 ◀
 제어판 검색 P 0 제어판 홈 컴퓨터의 시각 효과 및 소리 변경 바탕 화면 아이콘 변경 바탕 화면의 배경, 장 색, 소리 및 화면 보호기를 모두 한 번에 변경하려면 테마을 클릭하십 10 마우스 포인터 변경 내 테마 (1) 계정 사진 변경 저장하지 않은 테마 테마 저장 온라인으로 추가 테마 보기 Aero 테마 (7) Windows 7 조현물 캐릭터 참고 항목 디스플레이 작업 표시줄 및 시작 메뉴 바탕 화면 배경 장색 화면 보호기 소리 접근성 센터 빈 화면 슬라이드 쇼 회정 풍경
- 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 표시를 선택합니다.

💐 화면 보호기 설정
화면 보호기
-1 rs - 57 4,0000
2 0 0 År Å
n n n n n n n n n n n n n n n n n n n
· 0
화면 보호기(S)
AhnLab Screensaver
대기(W): 10 즉 부
전원 관리
성능을 최대화합니다.
<u>전원 설정 변경</u>
확인 취소 적용(A)

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 해제하기를 눌러 모든 사용자 공유 폴더를 해제하십시오.

점김 항목 상세 정보		
점검 결과: 취약	~	공유 폴더 해제하기
PC에 1개의 공유 폴더가 있습니다. ▶ [공유 폴더 해제하기]를 눌러 모든 사용자 공유 폴더를 해제하십시오.		
새 졸더		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 니다.	바랍	
	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

점검 결과가 취약인 경우 다음과 같이 조치하여 주시기 바랍니다.

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

사용자 공유 폴더 보기 - /	AhnLab 내PC지키미		X
공유 폴더 이름 새 폴더	폴더 경로 E:₩새 폴더		 _ <u>공유 폴더 해제</u> _
공유 졸더 설명			
		모	든 공유 폴더 해제
			달기

- 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
 삭제하기를 눌러 사용하지 않는 Active X 를 삭제합니다.

점검 항목 상세 정보		
점검 결과: 취약 PC에 90일 미상 사용하지 않은 ActiveX 프로그램이 1개 있습니다. ▶ [ActiveX 삭제하기]를 눌러 마래 ActiveX 프로그램을 삭제하십시오.	*	ActiveX 삭제하기
1, CQWebForKIPO Control		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
* ActiveX 프로그램이 삭제되지 않는 경우, 조치 방법 상세 안내 > FAQ를 참고하십시오.	Ŧ	<u>조치 방법 상세 안내</u>

한참고

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.

- 미사용 ActiveX 프로그램 존재 점검 항목에서 취약으로 진단된 경우 점검 항목 상세 정보 옆에 있는 ActiveX 삭제하기를 실행합니다.
- 미사용 ActiveX 프로그램 목록이 화면에 나타납니다. 목록에서 삭제할 대상을 선택한 후에 ActiveX 삭 제하기를 누릅니다.

7	ActiveX 프로그램 비를 CQWebForKIPO Control	마지막 사용 날짜 2014-06-24 13:26:04	다운로드 수소 C:₩PROGRA~1₩EPS₩KIPO₩CQWEBF~1.0CX
			ActiveX 삭제하기 정보

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

CQW	ebForKIPO Control	×
Г		
	CLSID	CQWebForKIPO Control
	파일 절대 경로	{63A7967F-5300-48FC-984B-16FC0D69BD99}
	다운로드 받은 사이트	http://www.patent.go.kr/ocx/CQWebForKIPO.cab
	게시자	{86FD811E-44E2-47AB-94C4-6CCF853B9ED1}
	인증자	CQWebForKIPO
	마지막 사용일	2014-06-24 13:26:04
		달기

3. 삭제 진행 과정이 표시되며, 삭제가 완료되면 확인을 눌러 창을 닫습니다.

ActiveX 프로그램 삭제 - AhnLab 내PC지키미					
ActiveX 프로그램 삭제를 마쳤습니다.	100%				
확인					

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 조치를 USB 자동 실행 기능을 해제하십시오.

점겸 항목 상세 정보		
점검 결과: 취약	*	위클릭 조치
USB 자동 실행을 사용하면 USB에 저장된 감염 파일을 통해 PC가 악성코드에 감염될 위험이 높아집니다. ▶ [자동 실행 차단하기]를 눌러 USB 자동 실행을 차단하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

한참고

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

조치 방법

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

[원클릭 조치]

- 1. 점검 항목 상세 정보에서 원클릭 조치를 누릅니다.
- 2. USB 자동 실행 차단이 설정되면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPCA	1710	X
i	USB 자동 실행을 차단했습니다. 확인	

3. 알림 창에서 확인을 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: PC에 비인가 프로그램이 설치되어 있지 않습니다.
- 취약: PC 에 설치된 비인가 프로그램의 목록이 나타납니다. 프로그램 삭제하기를 눌러 비인가 프로그램을 삭제하십시오.



조치 방법

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

비인가 프로그램 설치 점검의 점검 항목 상세 정보에 표시된 비인가 프로그램을 삭제하려면 프로그램
 삭제하기를 누릅니다.

점검 항목 상세 정보		
점검 결과: 취약 PC에 86개의 비인가 프로그램이 설치되어 있습니다. ▶ [프로그램 삭제하기]를 눌러 모든 비인가 프로그램을 삭제하십시오.	II	프로그램 삭제하기
1, Microsoft Lync - 환영합니다 localhost 2, A-Tuning v2,0,116,3 - 3, ASRock App Charger v1,0,6 - ASRock Inc. 4, ASRock SmartConnect v1,0,6 - ASRock Inc. 5, ASRock XFast RAM v3,0,3 - ASRock Inc. 6, ATnotes Version 9,5 - Thomas Ascher 7, Adobe AIR - Adobe Systems Incorporated 8, Adobe Flash Player 18 ActiveX - Adobe Systems Incorporated 9, Abol ab Opline Security - Abol ab Inc.	-	<u>조치 방법 상세 안내</u>

 제어판이 나타나면, 삭제 대상 프로그램을 선택하고 화면 상단의 제거나 변경을 눌러 해당 프로그램을 PC에서 삭제합니다.
ⓒ ♥ ◙ ▶ 제어판 ▶ 프로	그램 🕨 프로그램 및 기능	+ 4 7	프로그램 및 기능 검색
제어판 홈 설치된 업데이트 보기	프로그램 제거 또는 변경 프로그램을 제거하려면 목록에서 선택한 후 [제거], [변경	또는 [복구]를 클릭하십시오.	
함 함	구성 🕶 제거 변경		ji • 6
	이름	게시자	설치 날짜
	Microsoft .NET Framework 4.5.1	Microsoft Corporation	2014-08-06
	B 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
	C 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.

점검 항목 상세 정보		
점검 결과: 취약	*	
PC에 설치되지 않은 보안 USB가 있습니다.		
1. [HKEY_LOCAL_MACHINE₩SOFTWARE₩Wow6432Node₩Microsoft₩Windows 실치		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	÷	<u>조치 방법 상세 안내</u>

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 조치를 눌러 설치된 무선 랜카드를 제거하십시오.

점검 항옥 상세 성모		
점검 결과: 취약	*	원클릭 조치
PC에 2 개의 무선 랜카드가 설치되어 있습니다. ▶ 무선 랜카드는 설치할 수 없습니다. [원클릭 조치]를 눌러 설치된 무선 랜카드를 제거하십시오.		
<mark>무선 네트워크 연결 81</mark> (802,11 USB Wireless LAN Card #39) <mark>무선 네트워크 연결 82</mark> (Microsoft Virtual WiFi Miniport Adapter #43)		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

한참고

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

조치 방법

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

[원클릭 조치]

- 1. 점검 항목 상세 정보에서 원클릭 조치를 누릅니다.
- 2. 무선 랜카드를 삭제하면 다음과 같은 알림 창이 나타납니다.

AhnLab 내PC지키미	ALC: MIT: BIT: BIT:	
(1) 무선 랜키	는다가 모두 삭제되었습니다.	
	확인	

3. 알림 창에서 확인을 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.

Contraction of the second			
제어판 홈	프로그램 제거 또는 변경		
선치되 어데이트 비기			
2112 2119 - 21	프로그램을 세거아려면 폭독에서 진책한 후 [세거], [면경]	[또은 [복구]을 클릭아십시오.	
Williuuws 기능 사용/사용 인 항			
	구성 * 세거 변경		B== • (
	이름	게시자	설치 날짜
	Microsoft .NET Framework 4.5.1	Microsoft Corporation	2014-08-06
	Wicrosoft 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
	C Microsoft SQL Server Compact 3.5 SP2 ENU	Microsoft Corporation	2015-01-06
	C 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
	1 () III		

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.

점검 항목 상세 정보		
점검 결과: 취약	*	업데이트 설치하기
PC에 설치된 Acrobat Reader 11 (11.0.11.18)에 대한 최신 보안 업데이트를 설치해야 합니다. ▶ [업데이트 설치하기]를 눌러 Adobe 홈페이지에서 PDF 프로그램의 최신 보안 패치를 다운로드하며 업 데이트를 진행하십시오.		<u>Adobe 홈페이지</u>
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

점검 결과가 **취약**일 때, <u>APM 라이선스가 없는 경우</u>와 <u>APM 라이선스가 있는 경우</u>에 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 설치하기를 눌러 Adobe PDF 프로그램의 최신 보안 패치를 적용합니다.
- Adobe 홈페이지에 접속하여 최신 버전의 업데이트 파일을 다운로드 하여 설치합니다.



한참고

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.

점검 항목 상세 정보		
점검 결과: 취약 PC에 설치된 Acrobat Reader 11 (11.0.11.18)에 대한 최신 보안 업데이트를 설치해야 합니다. ▶ [업데이트 설치하기]를 눌러 Adobe 홈페이지에서 PDF 프로그램의 최신 보안 패치를 다운로드하며 업 데이트를 진행하십시오.	*	업데이트 설치하기 Adobe 홈페이지
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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

Ahn	Lab Patch Mana	gemei	nt			
적용	되지 않은 죄신 패	치가	18개	있습니다. 지금 적용하시겠싙	aLL 까?	
모두	보기 💌 1개	ዘ 선택	E		* <u>적용된 패치 목록</u> (t
	패치 분류	위형	성도	패치 변호	패치 이름	11
	일반 SW 패치	IIII	긴급	MS15-057	Windows Media Player의 취약성으로 인한 원격 코드 실행 문	
	일반 SW 패치	ш	중요	Adobe AIR	Adobe AIR Update (22.0.0.153)	
	일반 SW 패치		긴급	MS12-016	.NET Framework 및 Microsoft Silverlight의 취약점으로 인한	
	일반 SW 패치		긴급	MS12-025	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
	일반 SW 패치		긴급	MS12-035	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
	일반 SW 패치	1111	긴급	MS12-038	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
	일반 SW 패치	1111	긴급	MS12-045	Microsoft Data Access Components의 취약점으로 인한 원격	
	일반 SW 패치		긴급	HNC 2010	HNC 2010 업데이트 (000858)	
	일반 SW 패치		긴급	MS-KB2820331	Windows 7 및 Windows Server 2008 r 2에 대 한 응용 프로	
~	일반 SW 패치	Ш	긴급	Adobe Reader 10	Security updates for Adobe Reader and Acrobat (0010116)	
	일반 SW 패치		긴급	MS-KB2786081	로그 오프하거나 Windows 7 SP1 또는 Windows Server 200	
	일반 SW 패치	III	긴급	MS-KB2552343	Windows 7 또는 Windows Server 2008 R2가 실행되는 컴퓨	
	일반 SW 패치		긴급	MS-KB2813430	An update is available that enables administrators to update	
	일반 SW 패치	HH	긴급	MS13-053	Windows 커널 모드 드라미버의 취약점으로 인한 원격 코드	
	일반 SW 패치		긴급	MS13-057	Windows Media Format Runtime의 취약점으로 인한 원격 코	
	일반 SW 패치	m	38	M513-058	Windows Defender의 취약점으로 인한 권한 상승 문제점 (28	
	일만 SW 패지		88	JAVA SE Runtime Envir	JAVA SE Runtime Environment 8 (008092)	
	일만 SW 패지		긴급	Adobe Flash Player 14	Security updates available for Adobe Flash Player(APSB14-18)	
1				m		
					지금 업데이트 달기	

3. 지금 업데이트를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.

4. 패치 적용이 완료되면 화면 상단의 적용된 패치 목록을 눌러 설치된 패치 정보를 확인할 수 있습니다.

운영 체제 패치 운영 체제 패치 일반 SW 패치 일반 SW 패치 운영 체제 패치	••••	중요 기근	MS15-060			
운영 체제 패치 일반 SW 패치 일반 SW 패치 운영 체제 패치		기근		Microsoft 공용 컨트롤의 취약성으로 인한 원격	2015/06/09	1
일반 SW 패치 일반 SW 패치 운영 체제 패치	IIII		MS15-067	RDP의 취약성으로 인한 원격 코드 실행 문제(3	2015/07/14	
일반 SW 패치 운영 체제 패치		긴급	Adobe Reader 10	Security updates for Adobe Reader and Acrob	2015/10/13	
2영 체제 패치		긴급	MS-KB2533552	Windows 7 SP1, Windows Server 2008 R2 SP	2013/06/03	1
		긴급	MS-KB2861855	Microsoft 보안 공지: 원격 데스크톱 프로토콜	2013/08/13	
영 체제 패치		긴급	MS13-083	Windows 공용 컨트롤 라이브러리의 취약점으	2013/10/09	
2영 체제 패치		중요	MS-KB2731771	Windows 7 또는 Windows Server 현지 시간과	2012/10/08	
2영 체제 패치	m	중요	MS15-030	원격 데스크톱 프로토콜의 취약점으로 인한 서	2015/03/10	
				2 11 1		3

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 조치를 눌러 Windows 이벤트 로그를 덮어쓰지 않도록 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에 Windows 이벤트 로그를 덮어쓰기 하도록 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 Windows 이벤트 로그를 덮어쓰지 않도록 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. Windows 이벤트 로그를 덮어쓰기 하지 않도록 설정이 변경되면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC	
i	Windows 이벤트 로그를 덮어쓰기 하지 않도록 설정했습 니다.
	확인

3. 알림 창에서 확인을 누릅니다. 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

1. 작업 표시줄의 시작 > 컴퓨터에서 마우스 오른쪽 버튼을 클릭하여 관리를 선택합니다.

문사	1	And the second
사전	<u>1</u>	
음역	ł	
컴퓨	Ŧ터	
THO		열기(0)
410	۲	관리(G)
장치	۹ů	TortoiseSVN •
기년		네트워크 드라이브 연결(N)
		네트워크 드라이브 연결 끊기(C)
노코		바탕 화면에 표시(S)
		이름 바꾸기(M)
		속성(R)

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



- 3. <로그 속성>에서 최대 이벤트 로그 크기에 도달할 때의 옵션을 다음 2가지 중 1가지로 선택해야 합니다.
 - 로그가 꽉 차면 로그 보관. 이벤트를 덮어쓰지 않음
 - 이벤트 덮어쓰지 않음(수동으로 로그 지우기)

로그 속성 - 응용 프로그램	(유형: 관리)					
일반 구독						
전체 이름(E):	Application					
로그 경로(L):	%SystemRoot%#System32#Winevt#Logs#Application.evtx					
로그 크기:	20.00MB(20,975,616 바이트)					
만든 날짜:	2014년 8월 6일 수요일 오전 11:20:28					
수정한 날짜:	2015년 7월 22일 수요일 오전 8:56:16					
액세스한 날짜:	2014년 8월 6일 수요일 오전 11:20:28					
✓ 로깅 사용(E)						
최대 로그 크기(KB)(<u>X</u>): 20480 🔺					
최대 이벤트 로그 크기	기에 도달할 때:					
◎ 필요한 경우 이	벤트 덮어쓰기(가장 오래된 이벤트 먼저)(\\)					
◎ 로그가 꽉 차면	! 로그 보관. 이벤트를 덮어쓰지 않음(<u>A</u>)					
◎ 이벤트 덮어쓰지 않음(수동으로 로그 지우기)(N)						
	로그 지우기(<u>R</u>)					
	확인 취소 적용(P)					

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 조치를 눌러 사용자 계정 컨트롤(UAC) 사용을 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에 사용자 계정 컨트롤(UAC)이 설정되어 있지 않습니다. ▶ [원클릭 조치]를 눌러 사용자 계정 컨트롤(UAC) 사용을 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	-	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. UAC를 사용하도록 설정이 변경되면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC7	[7]D]
i	사용자 계정 컨트롤(UAC)을 사용하도록 설정했습니다.
	확인

3. 알림 창에서 확인을 누릅니다. 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

제어판의 사용자 계정에서도 UAC를 사용하도록 설정을 변경할 수 있습니다.

 Windows 작업 표시줄의 시작 > 설정 > 제어판 > 사용자 계정 및 가족 보호 > 사용자 계정을 선택한 후 사용자 계정 컨트롤 설정 변경을 선택합니다.

			Ξ <mark>Σ</mark>
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	세정 및 가족 모오 ▶ 사용사 세정 사용자 계정 변경 암호 제거 사진 변경 ☞ 계정 이를 변경 ☞ 계정 유형 변경 ☞ 다른 계정 관리 ☞ <u>사용자 계정 컨트롤 설정 변경</u>	▼ ♥ 제여관 검색 Annistrator 암호 사용	

2. 설정 값을 권장 값으로 올려줍니다.

😯 사용자 계정 컨트롤 설정		
컴퓨터 변경 내용(사용자계정 컨트롤은 유 <u>사용자계정 컨트롤 설정</u> 하사 악리	네 대한 알림 조건을 선택하십시오. 해한 프로그램이 컴퓨터를 변경하는 것을 방지하는 데 도움을 줍니다 <u>에 대한 자세한 내용 보기</u>	
	기본값 - 프로그램에서 사용자 모르게 컴퓨터를 변경하려 는 경우에만 알림(바탕 화면을 흐리게 표시) • 사용자가 직접 Windows 설정을 변경하는 경우 알리 지 않음	
- -	 이숙한 프로그램을 사용하거나 진숙한 웹 사이트을 방문하는 경우에 권장됩니다. 	
알리지 않음		
	· 🕅 확인	취소

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 조치를 눌러 보안 센터 서비스를 실행하십시오.

점검 항목 상세 정보		
점검 결과: 취약	^	원킄릭 조치
PC에 보안 센터 서비스가 실행되고 있지 않습니다. ▶ [원클릭 조치]를 눌러 보안 센터 서비스를 실행하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
		<u>조치 방법 상세 안내</u>
	-	

조치 방법

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

[원클릭 조치]

점검 결과가 취약인 경우 점검 항목 상세 정보에서 원클릭 조치를 눌러 보안 센터 서비스를 시작할 수 있습니다.

- 1. 점검 항목 상세 정보에서 원클릭 조치를 누릅니다.
- 2. 보안 센터 서비스를 시작하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC	지키미	23
i	보안 센터 서비스 실행을 마쳤습니다.	
	확인	

3. 알림 창에서 확인을 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.msc를 입력합니다.

📼 실행	22
	프로그램, 폴더, 문서 또는 인터넷 주소를 입력하십시오.
열기(<u>O</u>):	services.msc 🗸
	🛞 이 작업은 관리자 권한으로 실행됩니다.
	확인 취소 찾아보기(<u>B</u>)

2. 서비스 목록에서 Security Center를 확인합니다.

파일(F) 동작(A)	보기(V) 도움말(H)				
	Q 🛃 🛛 🖬 🖿 🖬 🖬 🕨				
💁 서비스(로컬)	· 서비스(로컬)				
	Security Center	이름	설명	상태	시작 유형
	서비스 <u>준지</u> 서비스 <u>다시 시작</u> 설명: WSCSVC(Windows 보안 센터) 서 비스는 컴퓨터의 보안 상태 설정 을 모니터링 및 보고합니다. 상태 설정에는 방화백(실정/재제), 바이 러스 백신 프로그림(설정/재제/만 로), 스파이웨어 방지 프로그림(설 정/해제/만료), Windows Update (자동 또는 수동으로 업데이트 다 운로드 및 설지), 사용자 계정 제어 (설정/재제) 및 인터넷 설정(권장/ 비권장)이 포함됩니다. 서비스는 ISV(Independent Software Vendor)에 COM API를 제공하여 제품 상태를 보안 센터 서비스에 등록 및 기록하도록 합니다. AC(관 리 센터) 미분 이 서비스를 사용하 여 시스템 트레이 경고 가능을 제 공하고 AC 제어판의 보안 상태를 그래픽으로 보여 준니다. NAPICI	Routing and Remote Access RPC Endpoint Mapper RSO3 MiddleTier Service Secondary Logon Secure Socket Tunneling Protocol Service Security Accounts Manager Security Center Server Shell Hardware Detection Smart Card Smart Card Smart Card Removal Policy SINMP Trap Software Protection SPP Notification Service SQL Server (SQLEXPRESS) SQL Server Active Directory Helper SQL Server VSS Writer SSQL Server VSS Writer SSDP Discrovery	로컬 영역 및 광역 네트워크 환경 끌점을 전송하기 위해 RPC 인터 내체 자격 중명 하에 프로세스를 VPN을 사용하여 원격 컴퓨터에 이 서비스의 시작은 보안 계정 관 에 정비스의 시작은 보안 계정 관 WSCSVC(Windows 보안 센터) 이 컴퓨터에 대해 파일. 인쇄 및 자동 실행 하드웨어 이벤트에 대 컴퓨터에서 스마트 카드를 액세 스마트 카드 제거 시 사용자 데스 로컬 또는 원격 SNMP(Simple N Windows 및 Windows 응용 프로 소프트웨어 라이션스 정품 인증 데이터의 저장, 처리 및 제어된 Active Directory와의 통합을 가 클라이언트 컴퓨터에 SQL Server Windows VSS 인프라를 통해 Mi IIPDP 자치아 관이 SCD P 거세 프	시작됨 시작됨 시작됨 시작됨 시작됨 시작됨	사용 안 함 자동 자동동 수동동 (10 함 여 (20 함))) (20 함 여 (20 함 여 (20 함 여 (20 함))) (20 함 여 (20 함 여 (20 함)) (20 함 (20 함)) (20 함) (20 함) (20 함)) (20 함) (20 ê) (20 ê) (

3. Security Center 서비스를 우클릭한 후 속성을 클릭합니다.

9 서비스			Contraction interest				-			x
파일(F) 동작(A)	보기(V) 도움말(H)									
	à 📑 🛛 🖬 🕨 💷 🕪									
🤐 서비스(로컬)	서비스(로컬)									
	Security Center		이름			설명		상태	시작 유형	*
	서비스 <u>중지</u> 서비스 <u>다시 시작</u>	^	 Routing and Remote Acces RPC Endpoint Mapper RSO3 MiddleTier Service 	s		로컬 영역 뜻 끝점을 전송	및 광역 네트워크 환경 하기 위해 RPC 인터	시작됨 시작됨	사용 안 함 자동 자동	
	설명: WSCSVC(Windows 보안 센터) 서 비스는 컴퓨터의 보안 산태 성정		Secondary Logon Secure Socket Tunneling P Security Accounts Manage	rotoo r	col Service	대체 자격 등 VPN을 사용 이 서비스의	증명 하에 프로세스를 하여 원격 컴퓨터에 I 시작은 보안 계정 관	시작됨	수동 수동 자동	
	비스는 컴퓨터의 보안 상태 설정 을 모니터링 및 보고합니다. 상태 설정에는 방화벽(설정/해제), 바이 러스 백신 프로그램(설정/해제)만 료), 스파이웨어 방지 프로그램(설 정/해제/만료), Windows Update (자동 또는 수동으로 업데이트 다 운로드 및 설치), 사용자 계정 제어 (설정/해제) 및 인터넷 설정(권장/ 비권장)이 포함됩니다. 서비스는 ISV(Independent Software Vendor)에 COM API를 제공하여 제품 상태를 보안 센터 서비스에 등록 및 기록하도록 합니다. AC(전 리 센터) 내는 이 서비스를 사용하 여 시스템 트레이 경고 기능을 제 공하고 AC 제어판의 보안 상태를 그래픽으로 보여 줍니다. NAP(네	E	Security Accounts Manage Security Center Server Shell Hardware Detection Smart Card Smart Card Removal Polic SmMP Trap Software Protection SPP Notification Service SQL Server (SQLEXPRESS) SQL Server Kowser SQL Server VSS Writer SQL Server VSS Writer SQL Server VSS Writer		시작(S) 중지(O) 일시 중지(계속(M) 다시 시작(모든 작업(새로 고침(속성(R) 도움말(H) ^{III}	U) E) K) ・	지역은 모안 세영 관 (ndows 보안 센터) 대해 파일, 인쇄 및 소마트 카드를 액세 지거 시 사용자 데스 일격 SNMP(Simple N Windows 응용 프로 같이선스 장품 인증 장, 처리 및 제어된 tory와의 통합을 가 컴퓨터에 SQL Server SS 인프라를 통해 Mi 와 관리 SSDP 거새 프	시작됨 시작됨 시작됨 시작됨 시작됨 시작됨	자중 자동(지연, 사용 안 함 자동 수동 수동 자동(지연, 수동 자동(지연, 사용 안 함 사용 안 함 사용 산 함	
로컬 컴퓨터에서 Secu	∖퐉쫑∕\#쑨/ ity Center 서비스를 시작합니다.									

4. 시작 유형을 자동으로 설정합니다.

Security Center 속성(로컬 컴퓨터)							
일반 로그온 복구 종속성							
서비스 이름: wscsvc							
표시 이름: Security Center							
설명: WSCSVC(Windows 보안 센터) 서비스는 컴퓨터의 보 🖕 안 상태 설정을 모니터링 및 보고합니다. 상태 설정에 🖕							
실행 파일 경로: C:₩Windows₩System32₩svchost,exe -k LocalServiceNetworkRestricted							
시작 유형(E): 자동							
<u>서비스 시작 옵션 구성 도움말</u>							
서비스 상태: 중지됨							
시작(S) 중지(T) 일시 중지(P) 계속(R)							
서비스를 시작할 때 적용할 시작 매개 변수를 지정할 수 있습니다.							
시작 매개 변수(M):							
확인 취소 적용(A)							

5. 이후 시작을 클릭하여 서비스를 시작합니다.

Se	urity Center 속성(로컬 컴퓨터)						
Γ	일반 로그온 복구 종속성						
L	서비스 이름: wscsvc						
L	표시 이름: Security Center						
l	설명: WSCSVC(Windows 보안 센터) 서비스는 컴퓨터의 보 안 상태 설정을 모니터링 및 보고합니다. 상태 설정에						
	실행 파일 경로: C:₩Windows₩System32₩svchost,exe -k LocalServiceNetworkRestricted						
L	시작 유형(E): 📉 🔨 🔻						
	서비스 시작 옵션 구성 도움말						
L	서비스 상태: 중지됨						
L	시작(S) 중지(T) 일시 중지(P) 계속(R)						
L	서비스를 시작할 때 적용할 시작 매개 변수를 지정할 수 있습니다.						
	서비스들 지작할 때 작용할 지작 매개 면수들 지정할 수 있습니다. 시작 매개 변수(M):						
L	확인 취소 적용(A)						

6. **확인**을 클릭하여 설정을 종료합니다.

Security Center 속성(로	리컬 컴퓨터) 📃 📉
일반 로그온 복	구 종속성
서비스 이름:	wscsvc
표시 이름:	Security Center
설명:	WSCSVC(Windows 보안 센터) 서비스는 컴퓨터의 보 안 상태 설정을 모니터링 및 보고합니다. 상태 설정에
실행 파일 경로: C:₩Windows₩Sy	ystem32₩svchost,exe -k LocalServiceNetworkRestricted
시작 유형(E):	자동 🗸
서비스 시작 옵션 -	<u>구성 도움말</u>
서비스 상태:	시작됨
시작(S)	중지(T) 일시 중지(P) 계속(B)
서비스를 시작할 [배 적용할 시작 매개 변수를 지정할 수 있습니다.
시작 매개 변수(M):
	확인 취소 적용(A)

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 조치를 눌러 Windows 자동 업데이트를 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	위클리 조치
PC에 Windows 자동 업데이트가 설정되어 있지 않습니다. ▶ [원클릭 조치]를 눌러 Windows 자동 업데이트를 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

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

[원클릭 조치]

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

- 1. 점검항목 상세 정보에서 원클릭 조치를 누릅니다.
- 2. 원클릭 조치로 Windows 자동 업데이트를 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC자 اال	3
(i) Windows 업데이트 설정을 자동 업데이트로 설정했습니 다.	1
확인	

3. 알림 창에서 확인을 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 startmenu를 입력합니다.

📼 실행	22
	프로그램, 폴더, 문서 또는 인터넷 주소를 입력하십시오.
열기(<u>O</u>):	wuapp.exe startmenu 👻
	🛞 이 작업은 관리자 권한으로 실행됩니다.
	확인 취소 찾아보기(<u>B</u>)

2. 좌측의 설정 변경을 클릭합니다.

● ● ▼ ▲ 제어판 → 모든 3	테어판 항목 ▶ Windows Update ▼ 4 제어판 검색	٩
제어판 홈	Windows Update	0
업데이트 확인 설정 변경 업데이트 기록 보기 숨겨진 업데이트 복원	Windows가 최신 상태입니다. 사용자 컴퓨터에 사용할 수 있는 업데이트가 없습니다.	
업데이트: 질문과 대답	최근 업데이트 확인: 오늘 오전 8:58 설치된 업데이트: 어제 오전 9:00. 업데이트 기록 보기 받을 업데이트: 시스템 관리자가 관리합니다. Windows Update에서 온라인 업데이트 확인	
참고 항목 설치된 업데이트		

3. 중요 업데이트 항목을 업데이트 자동 설치(권장)으로 설정 후 확인을 클릭합니다.

ⓒ ◯ ♥ 🖑 < 또 모든 제어판 항목 ▶ Windows Update ▶ 설정 변경	Q
	*
Windows에서 업데이트 설치 방법 선택	
🕕 일부 설정은 시스템 관리자가 관리합니다. 추가 정보	
컴퓨터가 온라인 상태인 경우 중요 업데이트를 자동으로 확인하고 이러한 설정을 사용하여 설치할 수 있습니 다. 또한 사용 가능한 새 업데이트가 있으면 설치한 후 컴퓨터를 종료할 수 있습니다. 자동 업데이트에 대한 자세한 정보	
중요 업데이트() ☑ 업데이트 자동 설치(권장)	Ξ
새 업데이트 설치(N): 매일 ▼ 시간(A) 오전 3:00 ▼	
권장 업데이트	
☑ 중요 업데이트를 받을 때와 같은 방식으로 권장 업데이트 제공(R)	
업데이트를 설치할 수 있는 사용자	
☑ 모든 사용자가 이 컴퓨터에 업데이트를 설치하도록 허용(U)	
참고: 업데이트를 확인할 때 먼저 Windows Update 프로그램 자체에 대한 업데이트가 필요할 수도 있습니다. 자세한 내용은 Microsoft의 <u>개인 정보 취급 방침</u> 을 참조하십시오.	-
🛞 확인 취소	

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 조치를 눌러 Administrators 그룹 내에 허가되지 않은 사용자 계정을 삭제하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에 Administrators 그룹에 허가되지 않은 사용자 계정이 있습니다. ▶ [원콜릭 조치]를 눌러 Administrators 그룹내에 허가되지 않은 사용자 계정을 삭제하십시오.		
Administrator		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	-	<u>조치 방법 상세 안내</u>

조치 방법

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

[원클릭 조치]

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

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

```
삭제하지 않으려면 아니요를 누릅니다.
```

AhnLab 내PC지키미	23
Administrators 그룹에 허가되지 않은 사용자 계정이 있습니다. Windows 기본 계정은 사용 안 함으로 변경하고, 그 외 허용되지 않은 계정은 삭제합니다. 계속 진행하시겠습니까?	
M OHLIB	

한참고

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 그룹을 선택합니다.

🌆 lusrmgr - [로컬 사용자 및 그룹(로	!컬)₩그룹]						x
파일(F) 동작(A) 보기(V) 도움	·말(H)						
🗢 🔿 🙍 🗊 🧟 🔒	Ī						
🐓 로컬 사용자 및 그룹(로컬)	이름	설명		-	작업		
사용자	Administrators	컴퓨터/도미	1인에 모든 액세스 권한을		그룹		•
	Backup Operators Cryptographic Operat Distributed COM Users Event Log Readers Guests IS_IUSRS Network Configuratio Performance Log Users Performance Monitor Power Users Remote Desktop Users Replicator Users SQLServer2005MSSQ SQLServer2005MSSQ	파일을 택입 구성원은 일 이 컴퓨터이 이 그룹의 · 기본적으로 인터넷 정말 이 그룹의 · 이 그룹의 · 이 그룹의 · 도메인에서 Users는 시: 해당 그룹의	G하거나 복원하기 위해 보안, 호화 작업을 수행할 권리가. I서 구성원이 DCOM 개체를 구성원은 로컬 컴퓨터에서 Users 그룹의 구성원과 동 실 서비스에서 사용하는 기본 구성원은 네트워크 기능의 구성원은 성능 카운터 로깅 구성원은 성능 카운터 데이 S는 이전 버전과의 호환성을 구성원은 원격으로 로그은할 파일 복제 지원 스템 수준 변경을 수행할 수 . 및 멤버에게 SQL Server 200 및 멤버에게 SQL Server 200	··· E		기타 작업	•
	SQLServer2005SQLBr	해당 그룹의	멤버에게 SQL Server 200	. •	·		

한참고

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

4. 그룹 폴더 내에 있는 Administrators 이름을 더블 클릭합니다.

파일(F) 동작(A) 보기(V) 도움 (추 🔿 🖄 🗊 🗙 🗐 🛃	음말(H) ? 🗊			
🕵 로컬 사용자 및 그룹(로컬)	이름	설명		작업
🎽 사용자	Administrators	컴퓨터/도메인에 모든 액세스 권한을		그룹 🔺
	Backup Operators	파일을 백업하거나 복원하기 위해 보안 구성원은 암호화 작업을 수행할 권리가		기타 작업 🕨
	A Distributed COM Users	이 컴퓨터에서 구성원이 DCOM 개체를		Administrators
	Event Log Readers Guests IIS_IUSRS Network Configuratio Performance Log Users Performance Monitor Power Users Remote Desktop Users Replicator Users SQLServer2005MSSQ SQLServer2005MSSQ	이 그룹의 구성원은 로컬 컴퓨터에서 기본적으로 Users 그룹의 구성원과 동 인터넷 정보 서비스에서 사용하는 기본 이 그룹의 구성원은 네트워크 기능의 이 그룹의 구성원은 성능 카운터 로깅 이 그룹의 구성원은 성능 카운터 데이 Power Users는 이전 버전과의 호환성을 이 그룹의 구성원은 원격으로 로그온할 도메인에서 파일 복제 지원 Users는 시스템 수준 변경을 수행할 수 해당 그룹의 멤버에게 SQL Server 200 해당 그룹의 멤버에게 SQL Server 200		기타 작업 ▶
	SQLServer2005SQLBr	해당 그룹의 멤버에게 SQL Server 200	Ŧ	<u> </u>

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

Administrators 속성	8	23
일반		
Administrators		
설명(E): 컴퓨터/도메인에 모든 액세스 권한을 가진 관리기 구성원(M):	71	
Mathematical Administrator		
추가(D) 제거(R) 사용자의 그룹 등록에 대한 변경 해당 사용자가 다음 번에 로그된 적용됩니다.	킹 내용 알 때	0
확인 취소 적용(A)	도움	말

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

Administrators 속성 양 전	3
일반	
Administrators	
설명(E): 컴퓨터/도메인에 모든 액세스 권한을 가진 관리자 구성원(M):]
See Administrator	
사용자의 그류 등록에 대한 변경 내용은	
체왕사용차가 다음 앤베 로크온할 때 적용됩니다.	
확인 취소 적용(A) 도움말	

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 조치를 눌러 LAN Manager 해시 값을 저장하지 않도록 보안 설정을 변경하십시오.

점검 항목 상세 정보		
점김 결과: 취약	^	원클릭 조치
PC에 패스워드의 암호화 알고리즘이 LAN Manager 해시 값을 저장하도록 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 보안 옵션을 변경하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
		<u>조치 방법 상세 안내</u>
	Ŧ	

조치 방법

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

[원클릭 조치]

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



3. 알림 창에서 확인을 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 조치를 눌러 장기간 미접속한 계정을 조치하십시오.

점검 항목 상세 정보		
점검 결과: 취약	^	원클릭 조치
PC에 30일 이상 미접속한 계정이 있습니다.(1개) ▶ [원클릭 조치]를 눌러 장기간 미접속한 계정을 조치하십시오.		
ahnlab2 - (마지막 접속 날짜:)		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 장기간 접속하지 않은 계정을 확인하고 원클릭 조치를 누릅니다.
- 다음과 같이 장기간 미접속 계정에 대한 처리 방식의 선택에서 예를 선택하면 Windows 기본 계정은 사용 안 함으로 변경하고, 그 외 계정은 삭제합니다. 아니요를 선택하면 설정을 변경하지 않습니다.



3. 알림 창에서 예를 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

점검 결과가 취약인 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.

AhnLab 내 PC 지키미 에이전트 사용설명서

🌆 lusrmgr - [로컬 사용자 및 그룹(5	2컬)]	
파일(F) 동작(A) 보기(V) 도울	}말(H)	
🏓 로컬 사용자 및 그룹(로컬)	이름	작업
🎽 사용자 🥂 🤭 그르	📫 사용자	로컬 사용자 및 그룹(로컬) 🔺
	🗎 그룹	기타 작업 🕨

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

💀 lusrmgr - [로컬 사용자 및 그룹(로	르컬)₩사용자]	_		
파일(F) 동작(A) 보기(V) 도움 < < 📄 🖄 💼 🔀	음말(H) ? 🗊			
🐓 로컬 사용자 및 그룹(로컬)	이름	전체 이름	작업	
- 사용사	🔩 Administrator		사용자	^
	<mark>전 Gliect</mark> 토 암호 설	정(S)	기타 작업	•
		91(K) b	Guest	^
	오는 작 작제(D) 이름 바· 속성(R) 도움말(I	열(K) 파가(M) H)	기타 작업	•
현재 선택한 항목을 삭제합니다.				

4. 예를 클릭하면, 사용자 계정이 삭제됩니다.



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

- 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 이름에는 삭제할 장기간 미접속 계정의 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 조치를 눌러 계정에 패스워드 사용 기간을 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약		원클릭 조치
PC에 4개의 계정이 패스워드 사용 기간이 설정되어 있지 않습니다. ▶ [원클릭 조치]를 눌러 패스워드 사용 기간을 설정하십시오.		
Administrator Guest ahnlab2		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.	•	<u>조치 방법 상세 안내</u>

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 패스워드 사용 기간이 설정되지 않은 계정을 확인하고 원클릭 조치를 누릅니다.
- 2. 취약 계정에 패스워드 사용 기간이 설정되고, 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

점검 결과가 취약인 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.

AhnLab 내 PC 지키미 에이전트 사용설명서

🅭 lusrmgr - [로컬 사용자 및 그룹(로컬)]					
파일(F) 동작(A) 보기(V) 도움	'말(H)				
 토컬 사용자 및 그룹(로컬) ▲ 사용자 ☐ 그룹 	이름 ^[1] 사용자 ^[1] 그룹	작업 로컬 사용자 및 그룹(로컬) ▲ 기타 작업 ▶			

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

🕵 lusrmgr - [로컬 사용자 및 그룹(회	르컬)₩사용자]			
파일(F) 동작(A) 보기(V) 도움	응말(H)			
	? 🗊			
 ◆ ● ▲ 2 ▲ 2 ▲ 2 ▲ 2 ▲ 48자 및 그룹(로컬) ● ● ● □ 	입 이름 전체 이름 정uest Guest MyPC MyPC test 단종 설정(S) 모든 작업(K) 삭제(D) 이름 바꾸기(M) 도움말(H) 조용말(H)	설명 컴퓨터/5 게스트가	<mark>작업</mark> 사용자 기타 작업 기타 작업	· · · · · · · · · · · · · · · · · · ·
현재 선택 내용에 대한 속성 대화 상	< <u>Ⅲ</u> 자를 엽니다.	•		

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

🚯 lusrmgr - [로컬 사용자 및 그룹(5	르컬)₩사용자]				X
파일(F) 동작(A) 보기(V) 도묻	}말(H)				
	? 🗊				
🐓 로컬 사용자 및 그룹(로컬)	이름	전체 이름	설명	작업	
· · · · · · · · · · · · · · · · · · ·	🛃 Administrator		컴퓨터/5	사용자	-
apc 속성				? ×	•
일반 소	속 그룹 프로필				•
	900			1	•
	apo				
전체 이름	(F): AhnLab)			
설명(D):					
	그온 시 사용자가 반!	드시 암호를 변경해야 함(M)		
· · · · · · · · · · · · · · · · · · ·	가 암호를 변경할 수 & 용 기간 제한 없음(Pi	없음(C))			
[용 안 함(B)				
┃ 계정 짐	겨 있음(0)				
		치소 저요/^			
		71 - 198(A			

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

- 시작 > 모든 프로그램 > 보조 프로그램에서 명령 프롬프트를 마우스 오른쪽 버튼으로 클릭하여, 관리자 권한으로 실행합니다.
- <명령 프롬프트>가 실행되면 다음과 같이 명령어를 입력합니다. 계정 이름에는 패스워드 사용 기간 제한을 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 함으로 설정하거나 원클릭 조치를 눌러 Guest 계정 이름을 변경하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에 Guest 계정 사용미 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 Guest 계정을 삭제하거나, 미름을 변경하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
		조치 바비 사세 아내
	-	<u> 포직 이미 이제 같네</u>

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 조치를 누릅니다.
- 알림 창에서 예를 선택하면 Guest 계정의 이름을 변경합니다. 아니요를 선택하면 계정 이름을 변경하 지 않습니다.



3. 예를 선택하면 Guest 계정의 이름을 변경하고 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

점검 결과가 취약인 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.

AhnLab 내 PC 지키미 에이전트 사용설명서

🌆 lusrmgr - [로컬 사용자 및 그룹(5	르컬)]	
파일(F) 동작(A) 보기(V) 도움	;말(H)	
 토컬 사용자 및 그룹(토컬) □ 사용자 □ 그룹 	이름 ⁶⁶ 사용자 ⁶⁶ 그룹	작업 로컬 사용자 및 그룹(로컬) ▲ 기타 작업 ▶
		,

 로컬 사용자 및 그룹 > 사용자를 클릭합니다. 목록에서 Guest 계정을 확인한 후, 마우스 오른쪽 버튼을 클릭하여 계정을 삭제하거나 이름을 변경해야 합니다.

🕭 lusrmgr - [로컬 사용자 및 그룹(최	르컬)₩사용자]	_			
파일(F) 동작(A) 보기(V) 도움말(H)					
🗢 🔿 🖄 📰 💥 🖻 🗟	? 🗊				
🐓 로컬 사용자 및 그룹(로컬)	이름	전체 이름		작업	
·····································	Administrator			사용자	^
	Guest	ahnlab	암	호 설정(S)	•
			모	든 작업(K) ▶	^
			삭	제(D)	•
			0	름 바꾸기(M)	
			속	성(R)	
			도	움말(H)	I
					I
					I
	< III		Þ	<u> </u>	

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

- 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 이름에는 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 함으로 설정된 계정의 개수가 나타납니다. 원클릭 조치를 눌러 사용 안 함 계정을 삭제하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에 사용 안 함 계정 1개가 있습니다. ▶ [원클릭 조치]를 눌러 사용 안 함 계정을 모두 삭제하십시오.		
ahnlab2		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	-	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 알림 창에서 예를 선택하면 Windows 기본 계정은 사용 안 함으로 변경하고, 그 외 계정은 삭제합니다.
 아니요를 선택하면 계정 정보를 변경하지 않습니다.



3. 알림 창에서 예를 선택하면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

점검 결과가 취약인 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.

💀 lusrmgr - [로컬 사용자 및 그룹(로컬)#사용자]					
파일(F) 동작(A) 보기(V) 도움말(H)					
🗢 🔿 🙋 📅 💥 🗒 😖 🛛	? 肩				
🐓 로컬 사용자 및 그룹(로컬)	이름	전체 이름	설명	작업	
□ 사용자 □ 고르	🛃 Administrator		컴퓨터/5	사용자	
	Suest	MURC	게스트가	기타 작업	•
	🔊 viyPC	test		조수민	
	🔬 арс	AhnLab		기타 작업	•
	•		F.		

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

AhnLab 내 PC 지키미 에이전트 사용설명서

🕭 lusrmgr - [로컬 사용자 및 그룹(로컬)\\사용자]					- • ×
파일(F) 동작(A) 보기(V) 도움말(H)					
🗢 🔿 🖄 🗔 🗙 🗐 🕹 🚺	? 🗊				
👰 로컬 사용자 및 그룹(로컬)	이름 전체	이름	설명	작업	
C 사용자 C 그르	🕵 Administrator		컴퓨터/5	사용자	
	Guest	~	게스트가	기타 작업	•
	💭 test test	C		조수민	_
	ap <u>r Abr</u>	ah		기타 작업	•
	암호 설정(·)			
	모든 작업() •			
	삭제(D)				
	이름 바꾸:	(M)			
	속성(R)				
	도운말(H)				
현재 선택한 항목을 삭제합니다.	•		•		

5. 예를 클릭하여 사용 안 함 계정을 삭제합니다.

🕭 lusrmgr - [로컬 사용자 및 그룹(5	로컬)₩사용자]			
파일(F) 동작(A) 보기(V) 도울	응말(H)			
🗢 🔿 🙋 📅 🗙 🗒 😖 🛽	? 🗊			
磿 로컬 사용자 및 그룹(로컬)	이름	전체 이름	설명	작업
□ 사용자 □ ㄱㄹ	🛃 Administrator		컴퓨터/5	사용자 🔺
- 그 늄	🛃 Guest	14.00	게스트가	기타 작업 🕨
	MyPC	MyPC		<u>x ~ n</u>
로컬 사용자	및 그룹			× •
	각 사용자 계정은 시 계정을 삭제하면 식 정을 만들어도 삭제 할 권한을 이미 가져 있습니다. apc 사용자를 삭제 ³	사용자 이름과 함께 고유 식별 별자도 삭제되며 똑같은 사 된 식별자를 복원할 수 없습 이고 있는 리소스에 대해 액서 하시겠습니까?	평자를 가집 용자 이름을 니다. 사용7 ∥스하지 못 [:] 예(Y)	니다. 사용자 : 가진 새 계 자는 액세스 하게 될 수도 아니요(N)
		111	4	

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.

▲ lusrmgr - [로컬 사용자 및 그룹(로컬)₩사용자]					
파일(F) 동작(A) 보기(V) 도움말(H)					
🗢 🔿 🖄 🗔 🗙 🗟 🖌	? 🗊				
磿 로컬 사용자 및 그룹(로컬)	이름	전체 이름	설명	작업	
□ 사용자 □ ㄱ=	🛃 Administrator		컴퓨터/5	사용자	
	🛃 Guest	14.00	게스트가	기타 작업	•
	🔊 MyPC	test		조수민	_
	🚛 арс	AhnLab		기타 작업	•
	•	III	4		

4. 활성화할 계정을 선택한 후, 마우스 오른쪽 버튼을 클릭하여 속성을 누릅니다.

♣ lusrmgr - [로컬 사용자 및 그룹(로컬)₩사용자]				
파일(F) 동작(A) 보기(V) 도움말(H)				
🗢 🔿 🖄 📰 🔀 🛛 🚺	2 📊			
로컬 사용자 및 그룹(로컬)	이름 전체 이름	설명 작업		
□ 시공시 □ 그룹	Standarinistrator	컴퓨터/되 사용자 게스트가	▲	
	MyPC MyPC	제프 제 기타 작업	•	
	test test		▲	
	🏜 암호 설정(S)	기타 작업	•	
	모든 작업(K) ▶			
	삭제(D)			
	이름 바꾸기(M)			
	속성(R)			
	도움말(H)			
현재 선택 내용에 대한 속성 대화 상	N를 엽니다.	r		

5. 계정 사용 안 함의 체크를 해제하고 확인을 클릭하여 해당 계정을 사용하도록 설정합니다.

🔊 lusrmgr - [로컬 사용자 및 그룹(5	[철)#사용자]
파일(F) 동작(A) 보기(V) 도울	말(H)
🛃 로컬 사용자 및 그룹(로컬)	이름 전체 이름 설명 작업
·····································	apc 속성
	일반 수송 그룹 프로필
	apc ·
	전체 이름(F): AhnLab
	설명(D):
	□ 다음 로그온 시 사용자가 반드시 암호를 변경해야 할(M) □ 사용자가 암호를 변경할 수 없음(C)
	☑ 암호 사용 기간 제한 없음(P) ☑ 암호 사용 기간 제한 없음(P)
	□ 계정 사용 안 합(B) □ 계정 잠겨 있음(O)
	확인 취소 적용(A) 도움말

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.
- <명령 프롬프트>가 실행되면 다음과 같이 명령어를 입력합니다.
 net user 계정 이름 /active:yes
 - 계정 이름에는 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 조치를 눌러 관리 Administrator 계정 이름을 변경하십시오.

점검 항목 상세 정보		
점겸 결과: 취약	^	원클릭 조치
PC에 Administrator 계정 사용이 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 Administrator 계정 이름을 변경하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 알림 창에서 예를 선택하면 Administrator계정의 이름이 변경되며, 아니요를 선택하면 계정 정보를 변 경하지 않습니다.

AhnLab LHPC7	۲(۶)D	23
4	Administrator 계정이 사용 중입니다. Administrator 계정을 Administrator_로 변경하시겠습니까? 예 아니요	

3. 알림 창에서 예를 선택하면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

점검 결과가 취약인 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.

🕭 lusrmgr - [로컬 사용자 및 그룹(로컬)]				
파일(F) 동작(A) 보기(V) 도움	숭말(H)			
록 ♥ ■ ■ ■ ■ 토컬 사용자 및 그룹(로컬)	이루	작업		
☐ 사용자 ☐ 그룹	· · · · · · · · · · · · · · · · · · ·	로컬 사용자 및 그룹(로컬) ▲		
	· 그룹	기타 작업		

 로컬 사용자 및 그룹 > 사용자를 클릭합니다. 목록에서 Administrator 계정을 확인한 후, 마우스 오른 쪽 버튼을 클릭하여 계정을 삭제하거나 이름을 변경해야 합니다.

🜆 lusrmgr - [로컬 사용자 및 그	[룹(로컬)₩사용자]				
파일(F) 동작(A) 보기(V)	도움말(H)				
🗢 🔿 🖄 🖬 📓	🛛 🖬				
💭 로컬 사용자 및 그룹(로컬)	이름	전체 이름	설명	작업	
□ 사용자 ◎ ㄱㄹ	👧 Administrator		커고티/티		^
	🕵 Guest		암오 실	EQ(S)	•
	S	anniab	모든 직	¦업(K) ▶	_
			삭제(D)	•
			이름 비	ŀ꾸기(M)	
			속성(R)	
			도운막	(H)	
					,
<	< <u> </u>		Þ		
사용자의 암호를 설정합니다.					

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

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

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

• 변경 이름에는 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.

점검 항목 상세 정보		
점검 결과: 취약 PC에 Windows 자동 로그온이 설정되어 있습니다. ▶[조치 방법 상세 안내]를 참고하며 Windows 자동 로그온 사용을 중지하십시오.	*	자동 로그온 해제
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 정보에서 자동 로그온 해제를 누릅니다.
- 2. 자동 로그온 해제를 위해 다음의 화면에서 Windows 로그온 패스워드를 입력하고 확인을 누릅니다.

Windows 자동 로그은 해제 - AhnLab 내PC지키미	<u> </u>
Windows 자동 로그온 기능을 해제하면, Windows 로그온 시 사용. 워드 입력이 필요합니다.	자 이름과 패스
Windows 로그온 패스워드를 입력하십시오.	
확인	취소

3. Windows 자동 로그온 기능 해제 알림 창이 나타납니다.

AhnLab 내PC지키	ונ	×
(i) wi	ndows 자동 로그온 기능이 해제되었습니다.	
	확인	

4. 알림 창에서 확인을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

윈도우의 사용자 계정에 자동으로 로그온 하도록 설정된 경우 다음과 같은 방법으로 설정을 해제할 수 있습니다. <u>사용자 계정을 통한 설정 변경</u>과 <u>레지스트리 수정/삭제를 통한 설정 변경</u>이 있습니다.

가. 사용자 계정을 통한 설정 변경

Windows 2003 이하

1. 윈도우 + R키를 눌러 실행 창을 띄운 후 control userpasswords2를 입력합니다.

실행			? ×
-	프로그램, 폴더, 문서 또	듣는 인터넷 리소스 이름	등을 입력하십시오.
열기(<u>0</u>):	control userpassword	ds2	_
	확인	취소	찾아보기(<u>B</u>)

2. 사용자 이름과 암호를 입력해야 이 컴퓨터를 사용할 수 있음을 체크 후 확인을 클릭합니다.

사용자 계정			? ×
[사용자] 고급			
사용자의 암호, 이 킬 ତ,	컴퓨터에 대한	권한, 기타 설정을 I	바꿀 수 있습니
✓ 사용자 이름과 암호를 입력 이 컴퓨터 사용자(U):	역해야 이 컴퓨터	터를 사용할 수 있을	i(E)
사용자 이름	·····································	er Users	
💽 vmuser	Admi	nistrators	
	±7K <u>D</u>)	제거(<u>B</u>)	속성(<u>0</u>)
약 하려면 물로 변경하려면 다 아이지 않는 말 한 아이지 않는 말 하려면 이 아이지 않는 아이 않는 아이지 않는	편 <ctrl+alt+de< td=""><td>▷을 누르고 [암호</td><td>변경]을 선택</td></ctrl+alt+de<>	▷을 누르고 [암호	변경]을 선택
		암호 다시	설정(<u>P</u>),,,
	확인	취소	적용(<u>A</u>)

Vista 이상

l. 윈도우	+ R 키를 눌러 실행 창을 띄운 후 netplwiz 를 입력합니다.
📼 실행	
	프로그램, 폴더, 문서 또는 인터넷 주소를 입력하십시오.
열기(<u>O</u>):	netplwiz 👻
	💱 이 작업은 관리자 권한으로 실행됩니다.
	확인 취소 찾아보기(<u>B</u>)

2. 사용자 이름과 암호를 입력해야 이 컴퓨터를 사용할 수 있음을 체크 후 확인을 클릭합니다.

사용자 계정
사용자 고급
사용자의 암호, 이 컴퓨터에 대한 권한, 기타 설정을 바꿀 수 있습니다.
☑ 사용자 이름과 암호를 입력해야 이 컴퓨터를 사용할 수 있음(E)
이 컴퓨터 사용자(山):
사용자 이름 그룹
Administrators
추가(D) 제거(R) 속성(O)
이 안후
~ 남호를 변경하려면 <ctrl+alt+del>을 누르고 [암호 변경]을 선 택하십시오.</ctrl+alt+del>
암호 다시 설정(만)
확인 취소 적용(<u>A</u>)

나. 레지스트리 수정/삭제를 통한 설정 변경

l. 윈도우-	+ R 키를 눌러 실행 창을 띄	운 후 regedit 를 입력합니다.
🖅 실행		×
	프로그램, 폴더, 문서 또는 인	인터넷 주소를 입력하십시오.
열기(<u>O</u>):	regedit	▼
	😚 이 작업은 관리자 권한의	으로 실행됩니다.
	확인	취소 <u>찾아보기(B)</u>

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

AhnLab 내 PC 지키미 에이전트 사용설명서

ProfileList	=(1)	이르	종류	GIOLEI
ProfileLoader			BEC C7	
ProfileNotification		ab Auto Admini agon	REG_SZ	(값 설명 안 됨)
		21 AutoAutimitEbgon	REG_32	0=0000001 (1)
👂 - 🔐 Schedule		ab Rackground	REG_DWORD	0.00000001(1)
D - Je SeCEdit		Background	REG_3Z	10
🔈 - 🍌 setup		ab Dobug Copyor Command	REG_SZ	10
SoftwareProtectionPl	atf	ab) DebugserverCommand	REG_3Z	abplab
p-		20 Deladitoserivarie	REG_SZ	anniab 0x00000001 (1)
Superfetch			REG_DWORD	0x00000001(1)
D- Svchost		The PorceOnlockLogon	REG_DWORD	0x0000000 (0)
SystemRestore		LeganvoliceCaption	REG_SZ	
p - Jerminal Server			REG_SZ	0.0000005 (5)
D - Ime Zones		PasswordExpiryWarning	REG_DWORD	0x00000005 (5)
b - in tracing		PowerdownAfterShutdown	REG_SZ	
Whom Ded		PreCreateKnownFolders	REG_SZ	{A520A1A4-1/80-4FF6-BD18-16/343C5AF16}
Windows		ReportBootOk	REG_SZ	1
Windows Activation	Ter	abscremoveoption	REG_SZ	0
Winlogon	iei	ab Shell	REG_SZ	explorer.exe
AutoLogonCheck	ed	ShutdownFlags	REG_DWORD	0x000002b (43)
GPExtensions		ab ShutdownWithoutLogon	REG_SZ	0
Winsat		ab Userinit	REG_SZ	C:#Windows#system32#userinit.exe,
WIDSATAPI		ab VMApplet	REG_SZ	SystemPropertiesPerformance.exe /pagefile
D WUDF		ab WinStationsDisabled	REG_SZ	0
windows Photo Viewer				
windows Portable Devices	*			

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

1(F)	편집(E)	보기(V)	즐겨찾기(A)	도움말(H)	[
		Þ-1	ProfileList	^	이름	종류	데이터
		P - 4	ProfileLoader		@)(기본값)	REG_SZ	(값 설정 안 됨)
		D 40	ProfileNotificat	on	ab AutoAdminLogon	REG_SZ	1
		Þ-1	Schedule	문자열 편집	5	80,24000	E E E E E E E E E E E E E E E E E E E
		D -	SeCEdit	710120	AIN:		
		Þ -]]	setup	값 미듬(
		D -]	SoftwareProtec	AUTOAD	minLogon		
		Þ-	SPP	값데이터	∃(⊻):		
61		D	Superfetch	U			15
		P - 3	SystemRestore	-		확인	취소
		b - 1	Terminal Server		· · · · · · · · · · · · · · · · · · ·		
		D -	Time Zones		200 PasswordExpiryWarning	REG_DWORD	0x00000005 (5)
		Þ -]	Tracing		ab PowerdownAfterShutdown	REG_SZ	0
			Userinstallable.	drivers	ab PreCreateKnownFolders	REG_SZ	{A520A1A4-1780-4FF6-BD18-167343C5AF16}
			WbemPerf		ab ReportBootOk	REG_SZ	1
			Windows		ab) scremoveoption	REG_SZ	0
		P -	Windows Activ	ation Tec	ab) Shell	REG_SZ	explorer.exe
		1 💚	Winlogon	Chacked	3 ShutdownFlags	REG_DWORD	0x000002b (43)
			GRExtension	пескеа	ab ShutdownWithoutLogon	REG_SZ	0
		P	Mincat	15	ab Userinit	REG_SZ	C:\Windows\system32\u00efuserinit.exe,
			WinSATADI		ab) VMApplet	REG_SZ	SystemPropertiesPerformance.exe /pagefile
		D-1	WUDF		ab WinStationsDisabled	REG_SZ	0
	Þ	Windo	ows Photo Viewe	r			
	Þ	Windo	ows Portable Dev	vices 🖕			
1 1	4 6						

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

📸 레지스트리 편집기	-	-	
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)			
Þ - D ProfileList	이름	종류	데이터
파일(P) 편집(E) 로/(V) 로/목갖/(A) 도움할(F) - ProfileLoader - ProfileLoader - ProfileNotification - FrofileNotification - Schedule - Schedule	이를 (기본건) AutoAdminLogon AutoRestartShell Background CachedLogonsCount DebugServerCommand DebugServ	종류 REG_SZ REG_DWORD REG_SZ	대이터 (값 설정 안 됨) 0 0x00000001 (1) 0 0 0 10 no abnlab 0000001 (1) 0000000 (0) 00000005 (5) 0 (A520A1A4-1780-4FF6-BD18-167343C5AF16) 1 0 explorer.exe 0x0000002b (43) 0 C:\#Windows\#system32\#userinit.exe, SystemPropertiesPerformance.exe /pagefile 0
Windows Proto Viewer			
• <u> </u>			
컴퓨터#HKEY_LOCAL_MACHINE#SOFTWARE#Microsof	t#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 조치를 눌러 패스워드의 최대/최소 사용 기간을 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에 패스워드 최대/최소 사용 기간이 설정되어 있지 않습니다. ▶ [원클릭 조치]를 눌러 패스워드의 최대/최소 사용 기간을 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
		T - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -
	-	<u>소지 망법 상세 안내</u>

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 조치를 누릅니다.
- 2. 관리자가 설정한 패스워드 최대/최소 사용 기간이 설정되면 다음과 같은 알림 창이 나타납니다.

AhnLab 내PC자	:[7]D]	23
i	패스워드 최대/최소 사용 기간 설정을 마쳤습니다. 최대 사용 기간: 90일 최소 사용 기간: 0일 확인	

3. 알림 창에서 확인을 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.

💷 실행	
	프로그램, 폴더, 문서 또는 인터넷 주소를 입력하십시오.
열기(0):	secpol.msc 🗸
	🚱 이 작업은 관리자 권한으로 실행됩니다.
	확인 취소 찾아보기(B)

2. 계정 정책 > 암호 정책을 클릭한 후 정책 목록을 확인합니다.



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

한참고

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 조치를 눌러 최근 사용한 패스워드를 저장하도록 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에 최근 사용한 패스워드 사용 여부를 점검하도록 설정되어 있지 않습니다. ▶ [원클릭 조치]를 눌러 최근 사용한 패스워드를 저장하도록 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

원클릭 조치 버튼을 통해 조치할 수 있습니다.

[원클릭 조치]

- 1. 점검항목 상세 정보에서 원클릭 조치를 누릅니다.
- 2. 관리자가 설정한 최근 사용한 패스워드 저장 개수가 사용자 PC에 설정되면 다음과 같은 알림 창이 나 타납니다.



3. 알림 창에서 확인을 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 조치를 눌러 계정 잠금을 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에 Windows 로그온 실패 횟수 초과 시 계정 잠금이 설정되어 있지 않습니다. ▶ [원클릭 조치]를 눌러 계정 잠금을 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	~	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치로 Windows 로그온 실패 횟수 초과 시 계정이 잠기도록 설정되면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC7	
i	Windows 로그온 실패 시 계정 잠금 설정을 마쳤습니다.
	확인

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 /s를 입력합니다.

📼 실행	22
	프로그램, 폴더, 문서 또는 인터넷 주소를 입력하십시오.
열기(<u>O</u>):	secpol.msc /s
	🚱 이 작업은 관리자 권한으로 실행됩니다.
	확인 취소 찾아보기(<u>B</u>)

2. 계정 정책의 하위에 있는 계정 잠금 정책에서 계정 잠금 임계 값을 더블 클릭합니다.

🚡 로컬 보안 정책		
파일(F) 동작(A) 보기(V) 도움말(H)		
🗢 🔿 🔁 📰 🗟 🖬		
보안 설정 실 계정 정책 실 약호 정책 실 약호 정책 실 약호 정책 실 감호 정책 실 고급 보안이 포함된 Windows 방화벽 네트워크 목록 관리자 정책 실 공개 키 정책 실 공개 키 정책 실 용 프로그램 제어 정책 실 양 IP 보안 정책(위치: 로컬 컴퓨터) 실 IP 보안 정책(위치: 로컬 컴퓨터) 실 고급 감사 정책 구성	정책 제정 잠금 기간 제 제정 잠금 임계값 제 지장 잠금 임계값 하다음 시간 후 계정 잠금 수를 원래대로 설정	보안 설정 적용할 수 없음 0 번의 잘못된 로그온 시도 적용할 수 없음
4		

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	adapte legs -	23
파일(F) 동작(A) 보기(V) 도움말(H		
🗢 🔿 🙋 💼 🗶 🗊 😖 🛛 🕫		
🖥 보안 설정	· 정책 · 보안 설정	
▲ 계정 정책 ▶ 아ㅎ 저채	🖏 계정 잠금 기간 적용할 수 없음	
이 지 하고 하지 않고 하지 하지 않는 하지 않고 하지 않는 하지 않고 않고 하지	····································	
▷ 🎇 로컬 정책	·····································	
▶ C 고급 보안이 포함된 Windows 방3	계정 잠금 임계값 속성 👘 🕺 🖄	
▶ 🛄 공개 키 정책	로컬 보안 설정 설명	
▷ 📫 소프트웨어 제한 정책	기정 잠금 임계값	
▶ — 응용 프로그램 세어 성색 ▶		
▷ 📫 고급 감사 정책 구성		
	다음 이후에 계정 잠금:	
	5 🚔 번의 잘못된 로그온 시도	
제안 값 변경		
	비값의 값이 지금 5 번의 잘못된 로그온 시도이므로, 다음 항목에 대한 설정이 제안 값으	
도 면정답니	r.	
정책	정책 설정 제안 설정 🔺	
📖 계정 잠	· 기간 적용할 수 없음 30 분 · · · · · · · · · · · · · · · · · ·	
	· 후 계성 삼금 수들 원래내로 석용발 수 없음 30 분 · · · · · · · · · · · · · · · · · ·	
	확인 취소(C)	
<	Þ	

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 조치를 눌러 다른 네트워크 사용자가
 PC 의 인터넷 연결 공유 기능을 사용할 수 없도록 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약 인터넷 연결(ICS) 공유 설정을 사용하고 있습니다. ▶ [원클릭 조치]를 눌러 다른 네트워크 사용자가 PC의 인터넷 연결 공유 기능을 사용할 수 없도록 설정 하십시오.	*	원클릭 조치
로컬 영역 연결		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

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

[원클릭 조치]

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

- 1. 점검항목 상세 정보에서 원클릭 조치를 누릅니다.
- 2. 원클릭 조치로 인터넷 연결 공유 설정을 해제하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC	עו≢וםן Σ	3
i	다른 네트워크 사용자가 에이전트 PC의 인터넷 연결을 통해 연결할 수 없도록 인터넷 연결 공유 설정을 해제하 였습니다.	
	확인	

3. 알림 창에서 확인을 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 센터로 이동합니다.
- 2. <네트워크 및 공유 센터>에서 어댑터 설정 변경을 누릅니다.



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



 <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 연 결할 수 있도록 허용(N)
홈 네트워킹 연결(H): 개인 네트워크 연결 선택 ▼
□ 다른 네트워크 사용자가 공유 인터넷 연결을 제어하거나 중지시킬 수 있도록 허용(0)
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 조치를 눌러 원격 사용자가 인증 없이 시스템 공유 디렉터리에 접속할 수 없도록 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
원격 사용자가 인증 없이 시스템 공유 디렉터리에 접속할 수 있게 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 원격 사용자가 인증없이 시스템 공유 디렉터리에 접속할 수 없도록 설정하십시 오,		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 원클릭 조치를 눌러 원격 사용자 인증 없이 시스템 공유 디렉터리에 접속할 수 없도록 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC7	۲ ۶ D <u>۲</u>
i	원격 사용자 인증없이 시스템 공유 디렉터리에 접속할 수 없도록 설정했습니다.
	확인

3. 알림 창에서 확인을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

- 1. 제어판에서 제어판 > 시스템 및 보안 > 관리 도구로 이동합니다.
- 2. <관리 도구>에서 로컬 보안 정책을 누릅니다.

-	And a state of the second			
중 ♥ ♥ 🔁 ▶ 제어판 ▶ 시	스템 및 보안 ▶ 관리 도구	▼ 4	리 도구 검색	م
구성 ▼ 🗊 열기 ▼	굽기			
☆ 즐겨찾기	이름	수정한 날짜	유형	크기
	desktop.ini	2014-08-06 오전	구성 설정	2KB
詞 라이브러리	🔝 iSCSI 초기자	2009 - 07-14 오후	바로 가기	2KB
	😹 Windows PowerShell Modules	2009-07-14 오후	바로 가기	3KB
1 컴퓨터	🔊 Windows 메모리 진단	2009-07-14 오후	바로 가기	2KB
	ᡒ 고급 보안이 포함된 Windows 방화벽	2009-07-14 오후	바로 가기	2KB
📬 네트워크	🔊 구성 요소 서비스	2009-07-14 오후	바로 가기	2KB
	📷 데이터 원본(ODBC)	2009-07-14 오후	바로 가기	2KB
	📠 로컬 보안 정책	2014-08-06 오전	바로 가기	2KB
	圖 서비스	2009-07-14 오후	바로 가기	2KB
	🔊 성능 모니터	2009-07-14 오후	바로 가기	2KB
	🔝 시스템 구성	2009-07-14 오후	바로 가기	2KB
	🔝 이벤트 뷰어	2009-07-14 오후	바로 가기	2KB
	歸 인쇄 관리	2014-08-06 오전	바로 가기	2KB
	🔊 작업 스케줄러	2009-07-14 오후	바로 가기	2KB
	🛃 컴퓨터 관리	2009-07-14 오후	바로 가기	2КВ
로컬 보안 정책 : 바로 가기	수정한 날짜: 2014-08-06 오전 11:22 만든 날짜 크기: 1.21KB	: 2014-08-06 오전 11:22	2	

- 3. <로컬 보안 정책>의 왼쪽 트리에서 로컬 정책의 보안 옵션을 선택합니다.
- 4. 오른쪽 화면에서 아래 정책 설정 값들의 보안 설정을 변경합니다.

🗄 로컬 보안 정책			x		
파일(F) 동작(A) 보기(V) 도움말(H)					
🗢 🔿 🙋 📰 🗟 🖬					
📑 보안 설정	^ ~	보안 설정	*		
▶ 🔄 계정 정책 ▲ 📆 로컬 정책	圆 네트워크 보안: 다음 암호 변경 시 LAN Manager 해시 값 저장 안 함	사용			
▷ 📴 감사 정책	颐 네트워크 보안: 로그온 시간이 만료되면 강제로 로그오프 颐 네트워크 보안: 로컵 시스템이 NTLM에 컴퓨터 ID를 사용하도로 허용	사용 안 암 정의되지 않음			
▶ <mark>고</mark> 사용자 권한 할당	🐻 네트워크 보안: 이 컴퓨터에 대한 PKU2U 인증 요청에서 온라인 ID를 사용하도록	정의되지 않음			
▶ 🧰 고급 보안이 포함된 Windows 방화벽	🖏 네트워크 액세스: Everyone 사용 권한을 익명 사용자에게 적용	사용 안 함			
🧰 네트워크 목록 관리자 정책	🚳 네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함	사용			
▶ 🛗 공개 키 정책	🛍 네트워크 액세스: SAM 계정의 익명 열거 허용 안 함	사용	=		
▷ 🧰 소프트웨어 제한 정책	🐻 네트워크 액세스: 네트워크 인증에 대한 암호 및 자격 증명의 저장소 허용 안 함	사용 안 함	-		
▷ 🧰 응용 프로그램 제어 정책	闘 네트워크 액세스: 로컬 계정에 대한 공유 및 보안 모델	<u>일반 - 로컬 사용.</u> .	. –		
▶ 🛃 IP 보안 정책(위치: 로컬 컴퓨터)	🚳 네트워크 액세스: 명명된 파이프와 공유에 대한 익명 액세스 제한	사용			
▶ 🚞 고급 감사 정책 구성	🖾 네트워크 액세스: 원격으로 액세스할 수 있는 레지스트리 경로	System#Current			
	🐻 네트워크 액세스: 원격으로 액세스할 수 있는 레지스트리 경로 및 하위 경로	System#Current			
1	闘 네트워크 액세스: 익명 SID/이름 변환 허용	사용 안 함			
	闘 네트워크 액세스: 익명으로 액세스할 수 있는 공유	정의되지 않음			
	📖 네트워크 액세스: 익명으로 액세스할 수 있는 명명된 파이프				
	🐻 대화형 로그온: [Ctrl+Alt+Del]을 사용할 필요 없음	정의되지 않음			
	B 대화형 로그온: 로그온을 시도하는 사용자에 대한 메시지 제목		-		

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

Ŀ	비트워크 액세스: Everyone 사용 권한을 익명 사용자에게 적용 속성 👘 🖓 📻 🏹
	로컬 보안 설정 설명
	네트워크 액세스: Everyone 사용 권한을 익명 사용자에게 적용
	◎ 사용(E)
	◉ 사용 안 함(S)
	확인 취소 적용(A)

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

네트워크 액서	네스: SAM 계정과 공유의 익명 열거 허용 안 함 속성 🛛 🔹 💻 🏹 🛁
로컬 보안	설정 설명
	네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함
<u>ا</u> لا (۲)	HB(E)
○ A	·용 안 함(S)
	D 설정을 수정하면 클라이언트, 서비스 및 응용 프로그램과의 호환성 에 영향를 미칠 수 있습니다. 자세한 내용은 <u>네트워크 액세스: SAM 계정과 공유의 익명 열거 허용</u> <u>안 함</u> 을(를) 참고하십시오. (Q823659)
	확인 취소 적용(A)

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

네트워크 액세스: SAM 계정의 익명 열거 허용 안 함 속성	? ×
로컬 보안 설정 설명	
네트워크 액세스: SAM 계정의 익명 열거 허용 안 함	
◎ 사용(E)	
◎ 사용 안 함(S)	
이 설정을 수정하면 클라이언트, 서비스 및 응용 프로그램과의 에 영향을 미칠 수 있습니다. 자세한 내용은 <u>네트워크 액세스: SAM 계정의 익명 열거 허용</u> (를) 참고하십시오, (Q823659)	호환성 <u>안 함</u> 을
확인 취소	적용(A)

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

Ŀ	비트워크 액세스: 명명된 파이프와 공유에 대한 익명 액세스 제한 속성 🛛 🔹 💌
	로컬 보안 설정 설명
	네트워크 액세스: 명명된 파이프와 공유에 대한 익명 액세스 제한
	● 사용(E)
	◎ 사용 안 함(S)
	확인 취소 적용(A)

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 조치를 눌러 무선 랜카드 사용을 중지하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에서 무선 랜카드를 사용하고 있습니다. ▶ [원클릭 조치]를 눌러 무선 랜카드 사용을 중지하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	-	<u>조치 방법 상세 안내</u>

조치 방법

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

[원클릭 조치]

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

AhnLab LHPC	지키미	23
i	무선 랜카드 사용을 중지했습니다.	
	확인	

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 조치를 눌러 비인가 사용자에 대한 접근을 허용하지 않도록 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에 비인가된 사용자(NULL Session)에 대한 접근 제어가 설정되어 있지 않습니다. ▶ [원클릭 조치]를 눌러 비인가 사용자의 접근을 제어하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치를 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 취약인 경우, 다음과 같은 방법으로 조치하여 주시기 바랍니다.

 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.)

AhnLab 내 PC 지키미 에이전트 사용설명서

해 레지스트리 편집기	-	Adventure furinger	MALENS AND	
파일(E) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)				
	*	이름	종류	데이터
FileSystem FileSystemUtilities FileSystemUtilitie	м — Ш	이름 (기본값) (기본값) () auditbasedirectories () auditbaseobjects () Authentication Packages () Cashonauditfail () disabledomaincreds () everyoneincludesanonymo () forceguest () forceguest () funtBlankPasswordUse () LisaPid () NoLmHash () NoLmHash () NoLmHash () NoLmHash () NoLmication Packages () ProductType () restrictanonymous () restrictanonymoussam	종류 REG_SZ REG_DWORD REG_DWORD REG_MULTI_SZ REG_BINARY REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	테이터 (값 설정 안 됨) 0x00000000 (0) 0x00000000 (0) msv1_0 00 30 00 00 02 000 00 0x00000000 (0) 0x00000000 (0) 0x00000000 (1) 0x00000001 (1) 0x00000001 (1) 0x00000001 (1) 0x00000001 (1) 0x00000001 (1)
Skew1		SecureBoot Security Packages	REG_DWORD REG_MULTI_SZ	0x00000001 (1) kerberos msv1 0 schannel wdigest tspkg
SSO	Ŧ	<		
컴퓨터\HKEY_LOCAL_MACHINE\SYSTEM\CurrentCon	trols	et#Control#Lsa		

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

DWORD(32비트) 값 편집	— X
값 이름(N): restrictanonymous	
값 데이터(V): 2	단위 한위 16진수(H) ③ 10진수(D)
	확인 취소

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 조치를 눌러 FTP 서비스를 중지하십시오.

점검 항목 상세 정보		
점검 결과: 취약	^	원킄릭 조치
PC에 FTP 서비스가 실행 중입니다. ▶ [원클릭 조치]를 눌러 FTP 서비스를 중지하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. FTP 서비스가 중지되고 다음과 같은 알림 창이 발생합니다.

AhnLab 내PC지키미	23
(Î) FTP 서비스를 중지했습니다.	
확인	

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

[사용자 조치]

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

이 서비스						×
파일(E) 동작(A)	보기(⊻) 도움말(出)					
(+ +) 🗊 🖸	Q 🛃 🛛 📷 🕨 🔳 💵 🕨					
🔍 서비스(로컬)	이 서비스(로컬)					
	Microsoft FTP Service	이름	설명	상태	시작 유형	다 ^
		🔍 Media Center Extender Service	Medi		사용 안 함	Lc
	서비스 중지 못	Microsoft .NET Framework NGEN v2.0.5	Micr	시작됨	자동(지연	Lc
	서비스 단지 시작	🖏 Microsoft FTP Service	비 서	시작됨	자동	Lc
		Microsoft ISCSI Initiator Service	이 컴		수동	Lc
	H.B.	Alicrosoft Software Shadow Copy Provider	볼륨		수동	Lc
	설명: 이 서버르 FTP(파익 저소 프로토콜)	i Multimedia Class Scheduler	시스	시작됨	자동	Lc
	서버로 사용하도록 설정합니다. 이 서	Net.Tcp Port Sharing Service	net.t		사용 안 함	LC
	비스를 중지하면 서버가 FTP 서버로	🔍 Netlogon	사용		수동	Lc =
	의 기능을 수행할 수 없습니다. 이 서	Network Access Protection Agent	NAP(수동	Ne
	비 비 프 글 시중에서 않도록 글장에진 된	Setwork Connections	네트	시작됨	수동	Lc
	다.	Ketwork List Service	컴퓨	시작됨	수동	LC
		Network Location Awareness	네트	시작됨	자동	Ne
		🐘 Network Store Interface Service	이 서	시작됨	자동	Lc
		NVIDIA Display Driver Service	Provi	시작됨	자동	LC
		NVIDIA Stereoscopic 3D Driver Service	Provi	시작됨	자동	LC
		NVIDIA Update Service Daemon	NVI	시작됨	자동(지연	.₩
		G Office Source Engine	업데		수동	Lc
		Gflice Software Protection Platform	Enab		수동	Nŧ
		Gfline Files	오프	시작됨	자동	Lc
		Parental Controls	이 서		수동	Lc ,
		✓ Ⅲ				*
	\확장∕표준∕					

3. 서비스 중지를 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 조치를 눌러 웹 서비스를 중지하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
PC에 웹 서버가 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 웹 서버 서비스를 중지하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.

2. World Wide Web Publishing Service 서비스가 중지되고 다음과 같은 알림 창이 발생합니다.

AhnLab 내PC지	[7]D]	<u> </u>
i	웹 서버 서비스를 중지했습니다.	
	확인	

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

[사용자 조치]

- Windows 작업 표시줄의 시작 > 설정 > 제어판 > 시스템 및 보안 > 관리 도구를 선택한 후, 서비스를 더 블 클릭하여 실행합니다.
- 2. 서비스 목록에서 World Wide Web Publishing Service를 선택합니다.
- 3. 서비스 중지를 눌러 World Wide Web Publishing Service 서비스를 중지합니다.

이 서비스	and in case		-		- 0 -	x
파일(F) 동작(A) !	보기(V) 도움말(H)					
	à 🛃 🛛 🖬 🖌 🗖 🖬 🖬					
💁 서비스(로컬)	Q 서비스(로컬)					
	World Wide Web Publishing	이름	설명	상태	시작 유형	
	Service 서비스 <u>중지</u> 서비스 <u>다시 시작</u> 설명: 인터넷 정보 서비스 관리자를 사용하 여 웹 연결 및 관리를 제공합니다.	 Windows Media Player Network Sharing Windows Modules Installer Windows Presentation Foundation Font Windows Process Activation Service Windows Remote Management (WS-M Windows Remote Management (WS-M Windows Search Windows Update Windows Update Windows VDdate Windows Config WLAN AutoConfig WMI Performance Adapter Workstation World Wide Web Publishing Service 	다른 일반 Wind 파일 네트 Wind Wind Wind Provi SMB 인터	시작됨 시작됨 시작됨 시작됨 시작됨 시작됨 시작됨	수동 수동동 수동동 수동동 자동(지연 수동 자동(지연 수동 수동 수동 수동 수동 수동 수동 자동 주동 자동 자동 자동 자동 자동 자동 자동 자동 구동 우동 우동 우동 우동 우동 우동 우동 우동 우동 우동 우동 우동 우동	
		WWAN AutoConfig	이 서		수동	4
		٠ (III			•	
	\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 조치를 눌러 Simple TCP/IP 서비스를 중지하십시오.

점검 항목 상세 정보		
점건 결과: 취약 PC에 Simple TCP/IP 서비스가 실행되고 있습니다. ▶ [원클릭 조치]를 눌러 Simple TCP/IP 서비스를 중지하십시오.	*	원클릭 조치
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
		<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. Simple TCP/IP 서비스가 중지되고 다음과 같은 알림 창이 발생합니다.

AhnLab LHPC	[지키]	23
i	Simple TCP/IP 서비스를 중지했습니다.	
	확민	

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

[사용자 조치]

- Windows 작업 표시줄의 시작 > 설정 > 제어판 > 시스템 및 보안 > 관리 도구를 선택한 후 서비스를 더블 클릭하여 실행합니다.
- 2. Simple TCP/IP Services 서비스를 중지합니다.

파일(E) 동작(A) 보기(V) 도운말(H)	이 서비스						X
····································	파일(E) 동작(A) !	보기(V) 도움말(H)					
서비스(로컬) Simple TCP/IP Services H비스 물직, 서비스 (로컬) Simple TCP/IP Services H비스 물직, 서비스 (로컬) Simple TCP/IP Services H비스 물직, 서비스 (로컬) Security Atting and Remote Access Remote Registry References Remote Registry Remote Rem	(+ +) 🗔 🖸	à 🔒 🛛 🖬 🖌 🗖 🖬 🕩					
Simple TCP/IP Services 이름 설명 상태 시작유형 다 서비스 즐지 서비스 댄스! 시조 유emote Registry 원격 수동 Lc 정비스 댄스! 시조 유emote Registry 원격 수동 Lc 성명: 다음 TCP/IP 서비스를 지원합니다: Secure Socket Tunneling Protocol Service VPN 수동 Lc 실명: 다음 TCP/IP 서비스를 지원합니다: Security Accounts Manager 이 서 시작됨 자동 Lc Character Generator, Daytime, Discard, Echo 및 Quote of the Day. Security Center WSC 시작됨 자동 Lc Security Center Security Center NSC 시작됨 자동 Lc Simple TCP/IP Services 다음 시작됨 자동 Lc Software Protection Wind <th>🔍 서비스(로컬)</th> <th>이 서비스(로컬)</th> <th></th> <th></th> <th></th> <th></th> <th></th>	🔍 서비스(로컬)	이 서비스(로컬)					
서비스 중지 서비스 열시 유지 서비스 인지 시작 응 Remote Registry 원격 수동 Lc 서비스 인지 시작 RPC Endpoint Mapper 끌점 시작됨 자동 N 설명: 다음 TCP/IP 서비스를 지원합니다: Character Generator, Daytime, Discard, Echo 및 Quote of the Day. Security Accounts Manager 이 서 시작됨 자동 Lc G Secure Socket Tunneling Protocol Service VPN 수동 Lc G Secure Socket Tunneling Protocol Service VPN 수동 Lc G Secure Socket Tunneling Protocol Service VPN 수동 Lc G Secure Socket Tunneling Protocol Service VPN 사용 안 함 Lc G Secure Socket Tunneling Protocol Service VPN 사용 안 함 Lc G Secure Socket Tunneling Protocol Service VPN 사용 안 함 Lc G Secure Socket Center VSC 시작됨 자동 Lc G Simple TCP/IP Services 다음 시작됨 자동 Lc G Software Protection Wind 시작됨 자동 Lc G SQL Server (MSSQLSERVER) 데이 시작됨 자동 N G SQL Server VSS Writer Wind 시작됨 자동 Lc		Simple TCP/IP Services	이름	설명	상태	시작 유형	다 ^
SQL Server VSS Writer Wind 시작됨 자동 Lc SSDP Discovery UPn 시작됨 수동 Lc (서비스 중지 서비스 <u>당시 시작</u> 설명: 다음 TCP/IP 서비스를 지원합니다: Character Generator, Daytime, Discard, Echo 및 Quote of the Day.	Remote Registry Routing and Remote Access RPC Endpoint Mapper Secondary Logon Secure Socket Tunneling Protocol Service Security Accounts Manager Security Accounts Security Acc	원격 로컬 끝점 대제 VPN 이 서 WSC 이 컴 자동 다음 로컬 Wind 소프 데이 Activ 클라	시작됨 시작됨 시작됨 시작됨 시작됨 시작됨 시작됨 시작됨	수동 사용 안 함 자동 수동 수동 자동(지연 사용 안 자동 주동 수동 주동 주동 주동 자동(지연 수동 자동(지연 수동 우동 가동 가동 가동 가동 가동 가동 가동 가동 가동 가동 가동 가동 가동	LC LC N LC LC LC LC LC LC N LC N N N N N
			SQL Server VSS Writer	Wind UPn	시작됨 시작됨	자동 수동	LC LC
			* <u> </u>	T 1 T 1			+
····································		\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 조치를 눌러 Windows 방화벽을 사용하도록 설정하십시오.

점검 항목 상세 정보		
점겸 결과: 취약	^	원클릭 조치
PC에 Windows 방화벽이 사용 안 함으로 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 Windows 방화벽을 사용하도록 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치를 눌러 Windows 방화벽을 사용하도록 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC	™ 121	×
i	Windows 방화벽을 사용하도록 설정했습니다.	
	확인	

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

[사용자 조치]

 Windows 작업 표시줄의 시작 > 설정 > 제어판 > 시스템 및 보안 > Windows 방화벽을 선택한 후 Windows 방화벽 설정 또는 해제를 선택합니다.

G	♥●♥♥ ♥ 제어판 ▶ 시스템	및 보안 🕨 Windows 방화벽	 ◄ ◀ 제어판 검색 	
	제어판 홈	Windows 방화벽을 사용하여 컴퓨터	보호	
	Windows 방화벽을 통해 프로 그램 또는 기능 허용	Windows 방화벽은 해커나 악성 소프트웨어가 인터 해 줍니다.	터넷 또는 네트워크를 통해 컴퓨터에 액세스하는 것을 방지	
8	알림 설정 변경	방화벽을 사용한 컴퓨터 보호 방법		
8	<u>Windows 방화벽 설정 또는 해</u> 제	네트워크 위치란?		
0	기본값 복원	📝 🧭 홈 또는 회사(개인) 네트워크(O) 연결되어 있지 않음 😒	
0	고급 설정	📝 공용 네트워크(P)	연결됨 🕥	
	네트워크 문제 해결			
		Windows 방화벽 상태:	설정	
		들어오는 연결:	허용되는 프로그램 목록에 없는 모든 프로그램 연결 차단	
	참고 항목	활성 공용 네트워크:	🇮 식별되지 않은 네트워크	
	관리 센터	알림 상태:	Windows 방화벽이 새 프로그램을 차단할 때 알림	
	네트워크 및 공유 센터			

 개인 네트워크일 경우 홈 또는 회사(개인) 네트워크 위치 설정의 Windows 방화벽 사용에, 공용 네트워크일 경우 공용 네트워크 위치 설정의 Windows 방화벽 사용에 체크 후 확인을 눌러 저장합니다.

CONTRACTOR AND
ⓒ ♥ 📾 ► 제어판 ► 시스템 및 보안 ► Windows 방화벽 ► 설정 사용자 지정 🔹 🍫 제어판 검색 👂
각 네트워크 유형의 설정을 사용자 지정합니다.
사용하는 각 네트워크 위치 유형의 방화벽 설정을 수정할 수 있습니다.
네트워크 위치란?
홈 또는 회사(개인) 네트워크 위치 설정 ● Windows 방화벽 사용 ■ 허용되는 프로그램 목록에 있는 연결을 포함하여 모든 들어오는 연결 차단 ▼ Windows 방화벽이 새 프로그램을 차단할 때 알림
😵 ── Windows 방화벽 사용 안 함(권장하지 않음)
공용 네트워크 위치 설정
◎ Windows 방화벽 사용 안 함(권장하지 않음)
확인 취소

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 조치를 눌러 원격 데스크톱 포트를 변경하십시오.

점검 항목 상세 정보		
점검 결과: 취약 PC에 원격 데스크톱 포트가 기본 포트(3389)로 설정되어 있습니다. ▶ [원콜릭 조치]를 눌러 원격 데스크톱 포트를 변경하십시오.	*	원클릭 조치
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치를 누르면 원격 데스크톱 포트가 기본 포트(3389)에서 변경되며, 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC7	AhnLab LHPCXI710				
i	원격 데스크톱 포트를 변경했습니다. 변경된 포트 번호: 7067				
	확인				

3. 알림 창에서 확인을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

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

 레지스트리 편집기를 열고 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp의 PortNumber를 더블 클릭하여 엽니다.

AhnLab 내 PC 지키미 에이전트 사용설명서

파일(F) 편집(E) 보기(V)	즐겨찾기(A) 도움말(H)	_			
파일(F) 편집(E) 보기(V) 	즐겨찾기(A) 도움말(H) KeyboardType Mapping RCM SessionArbitrationHelper SysProcs TerminalTypes Utilities VIDEO Wds WinStations Console EH-Tcp RDP-Tcp meZoneInformation ypm bflags bstor NN deo cncsvc df DI indows inlogon	* E	이를 OUBufDelay OutBufDelay OutBufDelay Password PdClass PdClass PdDLL PdDLL1 PdDLL1 PdFlag PdFlag PdFlag PdName PdName PdName PdName PdName PdName PdName PdName PdName OutSurdableProtocol_O PortNumber Shadow Shadow Shadow WdDLL WdPlag WdVame	客 류 REG_DWORD REG_SZ REG_DWORD REG_DWORD REG_SZ REG_DWORD REG_DWORD REG_SZ REG_DWORD REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ	E[[0]E] 0x00000064 (100) 0x000000212 (530) 0x00000002 (2) 0x00000000 (11) tdtcp tssecsrv 0x00000000 (0) tcp tssecsrv 0x00000000 (0) tcp tssecsrv 0x0000001 (1) 0x00000001 (1) 0x00000000 (0) rdpwd 0x00000036 (54) Microsoft RDP 7.1
	inresume		WUPICIA	NE0_52	NUP .

2. 10진수에 체크하고 변경할 포트 번호를 넣고 확인을 누릅니다.

DWORD(32비트) 값 편집	X
값 이름(N): PortNumber	
값데이터(V): 8888	단위 16진수(H) 10진수(D)
	확인 취소

 Windows 작업 표시줄의 시작 > 설정 > 제어판 > 시스템 및 보안 > Windows 방화벽을 선택한 후 고급 설정을 선택합니다.

🚱 🕞 ⊽ 🕍 🕨 제어판 ▸ 시스템	템 및 보안 ▶ Windows 방화벽	 ◄ 제어판 검색
제어판 홈	Windows 방화벽을 사용하여 컴퓨터	터 보호
Windows 방화벽을 통해 프로 그램 또는 기능 허용	Windows 방화벽은 해커나 악성 소프트웨어가 해 줍니다.	인터넷 또는 네트워크를 통해 컴퓨터에 액세스하는 것을 방지
🚱 알림 설정 변경	방화벽을 사용한 컴퓨터 보호 방법	
🛞 Windows 방화벽 설정 또는 해	네트워크 위치란?	
· · · · · · · · · · · · · · · · · · ·	🕑 🔮 홈 또는 회사(개인) 네트워크	크(O) 연결되어 있지 않음 📎
♥ 고급 설정 네트이크 모게 체경	😻 공용 네트워크(P)	연결됨 🐼
네드워그 군세 애널	공항 또는 커피숍과 같은 공공 장소의 네트워크	크입니다.
	Windows 방화벽 상태:	설정
	들어오는 연결:	허용되는 프로그램 목록에 없는 모든 프로그램 연결 차단
참고 항목	활성 공용 네트워크:	🇮 식별되지 않은 네트워크
관리 센터	알림 상태:	Windows 방화벽이 새 프로그램을 차단할 때 알림
네트워크 및 공유 센터		

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

🔐 고급 보안이 포함된 Windows 방화벽				
파일(F) 동작(A) 보기(V) 도움말((H)			
🗢 🄿 🙇 🖬 🗟 🖬				
로컬 컴퓨터의 고급 보안이 포함된	인바운드 규칙			작업
🔜 인마운드 규칙	이름	그룹	*	인바운드 규칙 🔺
이 것이군드 ㅠ넉	Ø APC.TCP.1433			🗱 새 규칙
▶ ▶ 모니터링	O APC.TCP.2002			▼ 프로필로 필터링
_	APC.TCP.2186			▼ 사태르 피터리
	ØAPC.TCP.2187			
	Ø APC.TCP.2191			▲ 그룹으로 필더당 ▶
	APC.ICP.5465			보기 🕨
	APC.TCP.3043			Q 새로 고침
	APC TCP 8952			🔜 목록 내보내기
	Ø APC.TCP.8953			
	@ APC.TCP.8954			
	Ø APC.TCP.8955			
	Ø APC6063			
	@ APC6178			
	@ APCLOG			
	MncCommCtrl TCP agent application		Ψ.	
	•	•		

5. 규칙 종류에서 **포트(O**)를 선택 후 다음을 누릅니다.
| 🔐 새 인바운드 규칙 마법사 | |
|---|---|
| 규칙 종류
만들려는 방화벽 규칙 종류를 선택합니 | LICF. |
| 달계: | |
| ● 규칙 종류 | 만들려는 규칙 종류는 무엇입니까? |
| 프로토콜 및 포트 작업 | 프로그램(P)
프로그램의 연결을 제어하는 규칙 |
| ● 프로필 | ◎ 王트(O) |
| ● 이름 | TCP 또는 UDP 포트의 연결을 제어하는 규척 |
| | © 미리 정의될(E):
BranchCache - 콘텐츠 검색(HTTP 사용) |
| | 사용자 지정 (C)
사용자 지정 규칙 |
| | 규칙 증류에 대해 자세히 알아봅니다. |
| | < 뒤로(B) 다음(N) > 취소 |

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

🔐 새 인바운드 규칙 마법사	
프로토콜 및 포트	
이 규칙을 적용할 프로토콜과 포트	를 지정하십시오.
당계: 규칙 종류 프로토콜 및 포트 작업 프로필 이름 	이 규착은 TCP에 적용됩니까, UDP에 적용됩니까? • UDP(U) 이 규칙은 모든 로컬 포트에 적용됩니까, 특정 로컬 포트에만 적용됩니까? • 모든 로컬 포트(A) • 특정 로컬 포트(S): 8888 예: 80, 443, 5000-5010
	프로토콜 및 포트에 대해 자세히 알아봅니다. (위로(B) [다음(N) > 취소

- 7. 작업에서 연결 허용을 선택합니다.
- 8. 프로필에서 다음과 같이 도메인, 개인, 공용에 모두 체크 표시한 후 다음을 클릭합니다.

	새 인바운드 규칙 마법사	
Ξ	도로필	
0	규칙을 적용할 프로필을 지정합니	LILF.
면	71:	
•	규칙 종류	이 규칙이 작용되는 시기는 언제입니까?
•	프로토콜 및 포트	
•	작업	컴퓨터가 회사 도메인에 연결된 경우 적용됩니다.
•	프로필	⑦ 개인(P)
•	이름	컴퓨터가 개인 네트워크 위치에 연결된 경우 적용됩니다.
		☑ 공용(U) 컴퓨터가 공용 네트워크 위치에 연결된 경우 적용됩니다.
		프로필에 대해 자세히 알아봅니다.

- 9. 이름에서 내용을 입력 후 **마침**을 누릅니다.
- 10. Windows 작업 표시줄의 시작 > 설정 > 제어판 > 시스템 및 보안 > 관리 도구를 선택한 후 서비스를 더 블 클릭하여 실행합니다.
- 11. Remote Desktop Services를 다시 시작합니다.

🔍 서비스						• X
파일(F) 동작(A) 보기(V) 도움말(H)						
🧼 🄿 🔲 🤉 🖬) 📝 🗊 🕨 🔲 II ID					
🔍 서비스(로컬)	🔍 서비스(로컬)	_				
	Remote Desktop Services	이름	설명	상태	시작 유형	다음 사용 ^
		Regram Compatibility Assistant Service	이 서	시작됨	자동	Local Sys
	서비스 중시 서자	🖏 Protected Storage	암호		수동	Local Sys
		🧠 Quality Windows Audio Video Experie	qWa		수동	Local Ser
		🧠 Remote Access Auto Connection Man	프로		수동	Local Sys
	설명: 사용자가 의견 커프티에 대하혀요르	Remote Access Connection Manager	이 컴		수동	Local Sys
	사용사가 원석 섬유니에 대와영우도 연결할 수 있습니다. 원격 데스크톸	Remote Desktop Configuration	RDC	시작됨	수동	Local Sys
	및 원격 데스크톱 세션 호스트 서버	Remote Desktop Services	사용	시작됨	수동	Network
	는 이 서비스에 종속됩니다. 이 컴퓨	Remote Desktop Services UserMode P	프린	시작됨	수동	Local Sys
	디의 원격 사용을 급시아더면 시스템 손성 제어판 항목의 [원격] 탭에 있는	Remote Procedure Call (RPC)	RPC	시작됨	자동	Network 📃
	확인란의 선택을 취소하십시오.	Remote Procedure Call (RPC) Locator	Wind		수동	Network
		Remote Registry	원격		수동	Local Ser
		Routing and Remote Access	로컬		사용 안 함	Local Sys
		RPC Endpoint Mapper	끝점	시작됨	자동	Network
		RSO3 MiddleTier Service		시작됨	자동	Local Sys
		Secondary Logon	대제		수동	Local Sys 👻
		•				+
	\확장/표준/					

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 조치를 눌러 원격 데스크톱 연결 설정을 해제하십시오.

점검 항목 상세 정보		
점검 결과: 취약 PC에 원격 데스크톱 연결을 허용하도록 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 원격 데스크톱 연결 설정을 해제하십시오.	*	원클릭 조치
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치를 눌러 원격 데스크톱 연결을 허용하지 않도록 설정하면 다음과 같은 알림 창이 나타납니다.



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

[사용자 조치]

 Windows 작업 표시줄의 시작 > 설정 > 제어판 > 시스템 및 보안 > 시스템을 선택한 후 고급 시스템 설 정을 선택합니다.

A REAL PROPERTY AND IN COLUMN			x
중 ♥ ♥ ♥ 제어판 ▶ 시스템	템 및 보안 ▶ 시스템	▼ 49 제어판 검색	P
제어판 홈	컴퓨터에 대한 기본 정	정보 보기	^
🚱 장치 관리자	Windows 버전		- 11
🚱 원격 설정	Windows 7 Enterprise K	\frown	
🚱 시스템 보호	Copyright © 2009 Micro	osoft Corporation. All rights reserved.	
♥ <u>고급 시스템 설정</u>	Service Pack 1		Ш
	시스템	_	_
	등급:	5.9 Windows 체험 지수	
참고 항목	프로세서:	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz 3.60 GHz	
관리 센터	설치된 메모리(RAM):	8.00GB(7.69GB 사용 가능)	
Windows Update	시스템 종류:	64비트 운영 체제	
성능 정보 및 도구	펜 및 터치:	이 디스플레이에 사용할 수 있는 펜 및 터치식 입력이 없습니 다.	Ŧ

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

시스템 속성
컴퓨터 이름 하드웨어 고급 시스템 보호 원격
원격 지원
☑ 이 컴퓨터에 대한 원격 지원 연결 허용(R)
원격 지원에 대한 정보
고급(\/)
원격 데스크톱
필요한 경우 옵션을 클릭한 다음 연결할 수 있는 사용자를 지정합니다.
◎ 미 컴퓨터에 대한 연결 허용 안 함(D)
 모든 버전의 원격 데스크톱을 실행 중인 컴퓨터에서 연 결 허용(보안 수준 낮음)(L)
◎ 네트워크 수준 인증을 사용하며 원격 데스크톱을 실행하는 컴퓨터에 서만 연결 허용(보안 수준 높음)(N)
선택 방법 사용자 선택(S)
· 확인 취소 적용(A)

3. 적용을 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 조치를 눌러 IE ActiveX 컨트롤 및 플러그 인 실행을 관리자 승인으로 설정하십시오.

점검 항목 상세 정보		
점겸 결과: 취약	*	원클릭 조치
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.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	-	<u>소지 방법 상세 안내</u>

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 조치를 누릅니다.
- 원클릭 조치를 눌러 IE ActiveX 컨트롤 및 플러그 인 실행을 관리자 승인으로 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC7	
i	IE의 ActiveX 컨트롤 및 플러그 인 실행을 관리자 승인으 로 설정하였습니다.
	확인

3. 알림 창에서 확인을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

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

6	새 탭	×	1 🖈 🗱
		인쇄(P)	1
		파일(F)	► [
		확대/축소(Z)	
		안전(S)	+
		시작 메뉴에 사이트 추가(M)	
		다운로드 보기(N)	Ctrl+J
		추가 기능 관리(M)	
		F12 개발자 도구(L)	
		고정된 사이트로 이동(G)	
		인터넷 옵션(O)	
		Internet Explorer 정보(A)	

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



ActiveX 컨트롤 및 플러그 인 실행에서 사용 설정 값을 제외한 설정 값을 선택합니다. 관리자 승인, 사용 안함, 확인 중에서 선택합니다.

보안 설정 - 인터넷 영역
설정
◎ 사용안함
.NET Framework 설치 사용
· · · · · · · · · · · · · · · · · · ·
◎ 사용 안 함 티
✔ ActiveX 컨트롤 및 플러그 인
● ActiveX 컨트롤 및 플러그 인 실행
◎ 관리자 승인
이 사용
◎ 차이
● 독신 ▲ ActiveX 컨트로옥 자동으로 사용자에게 화인
 ● 사용 안 함
● ActiveX 필터링 허용
◎ 사용
_ 🔘 사용 안 함 🚽
۲ (III) ا
*컴퓨터를 다시 시작해야 적용됩니다.
사용자 지정 설정
설정(R): 약간 높음(기본간) ▼ 위래대로(F)
확인 취소

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 조치를 눌러 IE 종료할 때 검색 기록을 삭제할 수 있도록 설정하십시오.

점검 항목 상세 정보		
점경 결과: 취약	*	원클릭 조치
▶ [원클릭 조치]를 눌러 IE 종료할 때 검색 기록을 삭제할 수 있도록 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치를 눌러 IE 종료할 때 검색 기록을 삭제하도록 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC	N710	
i	IE 종료할 때 검색 기록을 삭제하도록 설정하였습니다.	1
	확인	

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.

인터넷 옵션 양 🔀	
일반 보안 개인정보 내용 연결 프로그램 고급	
홈 페이지	
홈페이지 탭을 만들려면 한 줄에 하나씩 주소를 입력하십시오(R).	
·	
-	
현재 페이지(C) 기본값 사용(F) 새 탭 사용(U)	
시작 옵션	
◎ 마지막 세션의 탭으로 시작(B)	
◎ 홈 페이지로 시작(H)	
입사용에 관련된 옵션을 면영합니다. 법(I) 건생 기로	
입시 파일, 열어본 페이지 목록, 쿠키, 저장된 암호 및 웹 양식 정보를 삭 제합니다.	
▼ 종료할 때 검색 기록 삭제(W) 삭제(D) 설정(S) 모양	
색(O) 언어(L) 글꼴(N) 접근성(E)	
학인 취소 적용(A))

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 조치를 눌러 파일 다운로드 설정을 '사용 안 함'으로 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	원클릭 조치
IE 파일 다운로드가 가능하도록 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 파일 다운로드 설정을 '사용 안 함'으로 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치를 눌러 IE 파일 다운로드 기능을 사용 안 함으로 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC7	
i	IE 파일 다운로드 옵션을 사용하지 않도록 설정하였습니 다.
	확인

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.

인터넷 옵션 ? 💌 🏹
일반 보안 개인 정보 내용 연결 프로그램 고급
보안 설정을 보거나 변경할 영역을 선택하십시오.
인터넷 로컬 신뢰할수 제한된 인트라넷 있는 사이트 사이트 ▼
인터넷 사이트(S)
이 영역은 신뢰할 수 있는 사이트 및 제한된 사이 트에 포함된 웹 사이트를 제외한 인터넷 웹 사이트 를 위한 영역입니다.
이 영역에 적용할 보안 수준(L)
사용자 지정
사용자 지정 설정 - 설정을 변경하려면 [사용자 지정 수준]을 클릭하십시오. - 권장 설정을 사용하려면 [기본 수준]을 클릭하십시오.
▼ 보호 모드 사용(Internet Explorer를 다시 시작해야 함)(P)
사용자 지정 수준(C) 기본 수준(D)
모든 영역을 기본 수준으로 다시 설정(R)
확민 취소 적용(A)

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

보안 설정 - 인터넷 영역	x
설정	
◎ 사용 안 함	
□ 혼합된 콘텐츠 표시	
© \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	
○ ···· ◎ 사용 안 함	
· · · · · · · · · · · · · · · · · · ·	
₫ 다운로드	
🛃 글꼴 다운로드	
◎ 사용	
◎ 사용 안 함	
◎ 확인	
🛃 파일 다운로드	
◎ 사용	
④ 사용 안 함	
All 사용자 인증	
& 로그온	
◎ 사용자 이름 및 암호 확인	-
4 III +	
*컴퓨터를 다시 시작해야 적용됩니다.	
사용자 지정 설정	
·····································	
확인 취소	

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 조치를 눌러 사용자 이름/암호 자동 완성 기능을 해제하십시오.

점검 항목 상세 정보	
점검 결과: 취약	▲ 원클릭 조치
IE 에서 사용자 이름/암호 자동 완성 기능을 사용하고 있습니다. ▶ [원클릭 조치]를 눌러 사용자 이름/암호 자동 완성 기능을 해제하십시오.	
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 니다.	바랍
	<u>조치 방법 상세 안내</u> ▼

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 조치를 누릅니다.
- 2. 원클릭 조치를 눌러 IE 에서 사용자 이름/암호 자동 완성 기능을 사용하지 않도록 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC	
i	IE의 사용자 이름/암호 자동 완성 설정이 해제되었습니 다.
	확인

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 설정을 누릅니다.

인터넷 옵션
일반 보안 개인정보 내용 연결 프로그램 고급
가족 보호 설정
볼 수 있는 인터넷 콘텐츠를 제한합니다. 🔞 가족 보호 설정(F)
인증서
암호화된 연결 및 ID에 인증서를 사용합니다.
SSL 상태 지우기(S) 인증서(C) 게시자(B)
자동 완성
사용 완성은 이신에 입력한 내용 중에서 설정(I) 알맞은 내용을 추천해 줍니다.
비 피드 및 웹 조각
피드 및 웹 조각은 Internet Explorer와 기 설정(N) 타 프로그램에서 읽을 수 있는 웹 사이트
의 업데이트된 콘텐츠를 제공합니다.
· · · · · · · · · · · · · · · · · · ·

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 일 치하는 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

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.

점검 항목 상세 정보		
점검 결과: 취약	*	위클리 조치
IE ActiveX 컨트롤 다운로드 설정이 안전하지 않도록 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 IE ActiveX 컨트롤 다운로드 설정을 안전하게 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
		<u>조치 방법 상세 안내</u>
	Ŧ	

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 조치를 누릅니다.
- 2. 원클릭 조치를 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 확인으로 변경합니다.

AhnLab LHPC	
i	IE의 ActiveX 컨트롤 다운로드 설정을 확인으로 변경했 습니다.
	확인

3. 알림 창에서 확인을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

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

		-	
0	새 탭	×	🗄 🛠 🗱
-		인쇄(P)	Ī
		파일(F)	
		확대/축소(Z)	
		안전(S)	
		시작 메뉴에 사이트 추가(M)	
		다운로드 보기(N)	Ctrl+J
		추가 기능 관리(M)	
		F12 개발자 도구(L)	
		고정된 사이트로 이동(G)	
		인터넷 옵션(O)	
		Internet Explorer 정보(A)	

2. 보안 탭의 사용자 지정 수준을 클릭합니다.

인터넷 옵션 2 🗾 🗙
일반 보안 개인 정보 내용 연결 프로그램 고급
보안 설정을 보거나 변경할 영역을 선택하십시오.
인터넷 로컬 신뢰할 수 제한된 인트라넷 있는 사이트 사이트 ▼
인터넷 사이트(S)
이 영역은 신뢰할 수 있는 사이트 및 제한된 사이 트에 포함된 웹 사이트를 제외한 인터넷 웹 사이트 를 위한 영역입니다.
이 영역에 적용할 보안 수준(L)
이 영역에 어용된 수군, 모동-높음
- 약간 높음
- 대부분의 웹 사이트에 권장 - 잠재적으로 안전하지 않은 콘텐츠를 다운로드하기 전에 알림 - 서명되지 않은 ActiveX 컨트롤 다운로드 금지
▼ 보호 모드 사용(Internet Explorer를 다시 시작해야 함)(P)
사용자 지정 수준(C) 기본 수준(D)
모든 영역을 기본 수준으로 다시 설정(R)
확인 취소 적용(A)

 ActiveX 컨트롤 및 플러그 인 영역의 서명 안 된 ActiveX 컨트롤 다운로드/서명된 ActiveX 컨트롤 다운 로드를 권장으로 설정합니다.

보안 설정 - 인터넷 영역 📃 💌
설정
◎ 사용 안 함
● 바이너리 및 스크립트 동작
◎ 사용
◎ 사용안함
● 서명 안 된 ActiveX 컨트롤 다운로드
◎ 사용 (안전하지 않음)
 ● 사용 안 암 (권상) ● 화이
● 특근 ♥ 서명된 ActiveX 컨트롤 다운로드
◎ 사용 (안전하지 않음)
◎ 사용 안 함
● 왁인 (권상) ▲ 스크리트리 치요
 ▼ u = y, vis ○ A 8
● 사용 안 함
*컴퓨터를 다시 시작해야 적용됩니다.
사용자 지정 설정
설정(R): 약간 높음(기보간) ▼ 위래대로(F)
확인 취소

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 목록에 취약점이 존재하지 않습니다.
- 취약: IE 의 신뢰할 수 있는 사이트 목록에 신뢰할 수 없는 사이트의 URL 이 추가되어 있습니다. 원클릭 조치를 눌러 신뢰할 수 없는 사이트 URL 을 삭제하십시오.

점검 항목 상세 정보		
점검 결과: 취약 IE의 신뢰할 수 있는 사이트 목록에 신뢰할 수 없는 사이트 개가 추가되었습니다. ▶ [원클릭 조치]를 놓려 시리학 수 있는 사이트 IBI 을 삭제하십시오	*	원클릭 조치
ahnlab.com microsoft.com		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치를 눌러 설정을 변경하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC					
(1) 신뢰할 수 있는 사이트 목록에서 신뢰할 수 없는 사이트 URL을 모두 제거했습니다.					
	확인				

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

[사용자 조치]

1. Internet Explorer를 실행하여 도구 메뉴를 눌러 인터넷 옵션을 선택합니다.

일반 보안 개인 정보 내용 연결 프로그램 고급							
보안 설정을 보거나 변경할 영역을 선택하십시오.							
인터넷 로컬 신뢰할 수 제한된 인트라넷 있는 사이트 사이트 ·							
신뢰할 수 있는 사이트 사이트(S)							
이 영역에는 사용자 컴퓨터나 파일을 손상시키지 않을 것으로 신뢰되는 웹 사이트가 포함됩니다.							
이 영역에 웹 사이트가 있습니다. - 이 영역에 적용할 보안 수준(L) 이 영역에 허용된 수준: 모두							
- 보통 보통 안전하지 않은 콘텐츠를 다운로드하기 전에 알림 서명되지 않은 ActiveX 콘텐츠 다운로드 금지							
□ 보호 모드 사용(Internet Explorer를 다시 시작해야 함)(P)							
사용자 지정 수준(C) 기본 수준(D)							
모든 영역을 기본 수준으로 다시 설정(R)							
확인 취소 적용(A)							

3. 신뢰할수 없는 사이트를 클릭 후 제거를 누릅니다.

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

? ×



인터넷 옵션

인터넷 옵션 2 🔀
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
□ 이 영역에 있는 모든 사이트에 대해 서버 검증(https:) 필요(S)
달기(C)
10 10 TL(V)
모든 영역을 기본 수준으로 다시 설정(R)
확인 취소 적용(A)

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 조치를 눌러 사용자 인증 시 자동으로 로그인하지 않도록 설정하십시오.

점김 항목 상세 정보		
점검 결과: 취약	^	원클릭 조치
IE에서 사용자 인증 시 자동으로 로그인하지 않도록 설정되어 있습니다. ▶ [원클릭 조치]를 눌러 사용자 인증 시 자동으로 로그인하지 않도록 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
		<u>조치 방법 상세 안내</u>
	Ŧ	

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 조치를 누릅니다.
- 원클릭 조치를 눌러 사용자 인증 로그온 시, 사용자 이름과 암호를 확인하도록 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC	
i	IE에서 사용자 인증 시 자동으로 로그온 하지 않도록 설 정했습니다.
	확인

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(<u>C</u>)...**을 클릭합니다.



3. 사용자 인증 영역의 사용자 이름 및 암호 확인을 클릭 후 확인을 누릅니다.

보안 설정 - 인터넷 영역 📃 🗾
설정
◎ 사용 ▲
◎ 사용 안 함
○ 확인
🛃 🛃 파일 다운로드
◎ 사용
◎ 사용 안 함
👪 사용자 인증
<u>용 로그온</u>
◎ 사용자 이름 및 암호 확인
이 약영 도그온
◎ 천교 사용자 이르 및 양승은 사용치에 자동으로 르그의
·····································
Active ∧∃린틴
● \AB
◎ 사용 안 함 🗸
4 III +
*컴퓨터를 다시 시작해야 적용됩니다.
사용자 지정 설정
설정(R): 야가 노으(기보가) ▼ 의래대로(F)
확인 취소

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 조치를 눌러 IE 종료 시 임시 파일을 삭제하도록 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	^	원클릭 조치
IE 종료 시 임시 파일 삭제 설정이 되어 있지 않습니다. ▶ [원클릭 조치]를 눌러 IE 종료 시 임시 파일을 삭제하도록 설정하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치를 눌러 IE 종료 시 임시 인터넷 파일을 삭제하도록 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab 내PC지ㅋ	70	23
í I	IE 종료 시 임시 파일을 삭제하도록 설정했습니다.	
	확인	

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

[사용자 조치]

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

인터넷 옵션	? <mark>x</mark>							
일반 보안 개인정보 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 ● 입 암호화된 페이지를 디스크에 저장 안 함 ■ ■ 엄격한 P3P 유효성 검사 사용* ■ ▼ 민증서 주소가 일치하지 않은 경우에 경고* ▼								
	F.							
*컴퓨터를 다시 시작해야 적용됩니다. 고급 설정 복원	<u>(R)</u>							
Internet Explorer 기본 설정 복원								
Internet Explorer의 설정을 기본 상태대로 다시 설정 원래대로(S) 합니다.								
브라우저가 사용 불가능한 상태에 있을 때에만 이 기능을 사용해야 힘	합니다.							
<u>확인</u> 취소	적용(<u>A</u>)							

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 설치하기를 눌러 최신 버전의 보안 업데이트를 설치하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	업데이트 설치하기
Adobe Flash Player가 최신 업데이트 상태가 아닙니다. (현재 버젼: 18,0,0,232) ▶ 최신 버젼인 19,0,0,185로 업데이트하시기 바랍니다.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

점검 결과가 **취약**일 때, <u>APM 라이선스가 없는 경우</u>와 <u>APM 라이선스가 있는 경우</u>에 따라 다음과 같이 조치하여 주시기 바랍니다.

[APM 라이선스가 없는 경우]

- 1. 점검 항목 상세 정보에서 업데이트 설치하기를 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.

점검 항목 상세 정보		
점검 결과: 취약	^	업데이트 설치하기
Adobe Flash Player가 최신 업데이트 상태가 아닙니다. (현재 버전: 18,0,0,232) ▶ 최신 버전인 19,0,0,185로 업데이트하시기 바랍니다.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
		<u>조치 방법 상세 안내</u>
	Ŧ	

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

	패치 분류	위호	비도	패치 변호	패치 이름
	일반 SW 패치		긴급	MS15-057	Windows Media Player의 취약성으로 인한 원격 코드 실행 문
~	일반 SW 패치		긴급	MS12-016	.NET Framework 및 Microsoft Silverlight의 취약점으로 인한
~	일반 SW 패치		긴급	MS12-025	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
~	일반 SW 패치		긴급	MS12-035	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
~	일반 SW 패치		긴급	MS12-038	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
~	일반 SW 패치		긴급	MS12-045	Microsoft Data Access Components의 취약점으로 인한 원격
~	일반 SW 패치		긴급	MS-KB2820331	Windows 7 및 Windows Server 2008 r 2에 대 한 응용 프로
~	일반 SW 패치		긴급	MS-KB2786081	로그 오프하거나 Windows 7 SP1 또는 Windows Server 200
~	일반 SW 패치		긴급	MS-KB2552343	Windows 7 또는 Windows Server 2008 R2가 실행되는 컴퓨
~	일반 SW 패치		긴급	MS-KB2813430	An update is available that enables administrators to update
~	일반 SW 패치		긴급	MS13-053	Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드
~	일반 SW 패치		긴급	MS13-057	Windows Media Format Runtime의 취약점으로 인한 원격 코
~	일반 SW 패치	ш	중요	MS13-058	Windows Defender의 취약점으로 인한 권한 상승 문제점 (28
~	일반 SW 패치		긴급	Adobe Flash Player 14	Security updates available for Adobe Flash Player(APSB14-18)

- 3. 지금 업데이트를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.
- 4. 패치 적용이 완료되면 화면 상단의 적용된 패치 목록을 눌러 설치된 패치 정보를 확인할 수 있습니다.

태치 분류	위호	험도	패치 번호	패치 이름	패치 발표일	패치 설치
운영 체제 패치	ш	중요	MS15-060	Microsoft 공용 컨트롤의 취약성으로 인한 원격	2015/06/09	
일반 SW 패치		긴급	Adobe Flash Playe	Security updates available for Adobe Flash Pla	2015/08/11	2016/06
운영 체제 패치		긴급	MS15-067	RDP의 취약성으로 인한 원격 코드 실행 문제(3	2015/07/14	TEP-STREET, STREET, ST
일반 SW 패치		중요	Adobe AIR	Adobe AIR Update (22.0.0.153)	2016/06/16	2016/06
일반 SW 패치		긴급	HNC 2010	HNC 2010 업데이트 (000858)	2016/04/19	2016/06
일반 SW 패치		긴급	Adobe Reader 10	Security updates for Adobe Reader and Acrob	2015/10/13	2016/06
일반 SW 패치		긴급	MS-KB2533552	Windows 7 SP1, Windows Server 2008 R2 SP	2013/06/03	
운영 체제 패치	1111	긴급	MS-KB2861855	Microsoft 보안 공지: 원격 데스크톱 프로토콜	2013/08/13	
운영 체제 패치		긴급	MS13-083	Windows 공용 컨트롤 라이브러리의 취약점으	2013/10/09	
일반 SW 패치		중요	JAVA SE Runtime	JAVA SE Runtime Environment 8 (008092)	2016/04/20	2016/06
운영 체제 패치	m	중요	MS-KB2731771	Windows 7 또는 Windows Server 현지 시간과	2012/10/08	
운영 체제 패치	ш	88	MS15-030	원격 데스크톱 프로토콜의 취약점으로 인한 서	2015/03/10	
				111		

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 조치를 눌러 데이터 실행 방지(DEP) 기능을 사용하도록 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약 데이터 실행 방지(DEP) 기능을 사용하지 않고 있습니다. ▶ [원클릭 조치]를 눌러 데이터 실행 방지(DEP) 기능을 사용하도록 설정하십시오.	*	원클릭 조치
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	~	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치를 눌러 데이터 실행 방지(DEP)기능을 사용하도록 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC7	
i	데이터 실행 방지(DEP) 기능을 사용하도록 설정했습니 다.
	확인

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

[사용자 조치]

- 시작 > 모든 프로그램 > 보조 프로그램에서 명령 프롬프트를 마우스 오른쪽 버튼으로 클릭하여, 관리 자 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 AlwaysOff으로 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 실행하기를 눌러 다음 안전 조건을 준수하여 PC 내에 처리되지 않은 개인 정보 파일을 처리하십시오.

점겸 항목 상세 정보		
점검 결과: 취약 PC에 137개의 처리되지 않은 개인 정보 파일미 있습니다. ▶ [프로그램 실행하기]를 눌러 다음 안전 조건을 준수하여 PC 내에 처리되지 않은 개인 정보 파일을 처 리하십시오	•	프로그램 실행하기
총 미처리 파일 : 1개 미만 위험 파일: 1 개 미만 경고 파일: 1 개 미만 주의 파일: 1 개 미만	H	
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.	-	<u>조치 방법 상세 안내</u>

조치 방법

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

- 1. 점검 항목 상세 정보에서 프로그램 실행하기를 누릅니다.
- 2. 프로그램 실행하기를 누르면 다음과 같이 AhnLab Privacy Management Agent 가 실행됩니다.

AhnLab Priv	acy Management	Agent			-	
Home	검색 결과	격리	암호화	예외 처리	프로그램 차단	C 🕲 🗘 🕲
개인 경 개인 정 위험 경고 [주의	정보 검색 현 보 포함 정도에 (48 2 60	황 따라 검색 결과를 120	분류합니다. 181 180			개인 정보 유출 담지 현황 개의 정보 포함 문서가 유출되 지 양도록 보호합니다. 최근 7일간 탐지 횟수
개인정	보 처리 현황	⊙ 처리 10	(격리: 1, 암호화	: 9, 예외 처리: 0) 💌 미처리 2	31
可包 名	[색 수	운전면향 주민변호 외국인 등 검색된 표	번호 : 11,830 : : 459 등록변호 : 434 대턴별 파일 보기			

- 3. 개인정보 처리 현황에서 격리, 암호화, 예외 처리가 되지 않은 미처리 개인 정보 파일을 확인합니다.
- 4. 미처리 파일의 특성에 따라 격리, 암호화, 예외 처리를 합니다.

한 한 고

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. 처리하기를 눌러 PC 내에 처리되지 않은 개인 정보 파일을 처리하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	처리하기
PC에 239개의 처리되지 않은 개인 정보 파일이 있습니다. ▶ [처리하기]를 눌러 다음 안전 조건을 준수하여 PC 내에 처리되지 않은 개인 정보 파일을 처리하십시오		
총 미처리 파일 : 150개 미만 위험 파일: 10 개 미만 경고 파일: 15 개 미만 주의 파일: 55 개 미만		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

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

- 1. 점검 항목 상세 정보에서 처리하기를 누릅니다.
- 2. 처리하기를 누르면 다음과 같이 개인 정보 검색 창이 실행됩니다.

진	1행률 : 0% =====			-012 20				감색 중
	위협(0)	경고(1	4)	주의(228)			
11	파일 이름	검	색 패턴	검색 수	III-S	# 경로	수정 시간	탐지 시간
	외국인 등록번호	+	1종류	1	-	C:₩Users₩YongHun₩D	2014-06-09 15:55:50	2016-06-24 18:05:1
	Q 외국인 등록변호	. +	184	1	-	C:#Users#YongHun#D	2014-06-09 15:55:50	2016-06-24 18:05:1
	Q 외국인 등록번호	+	185	1		C:#Users#YongHun#D	2014-06-09 15:55:50	2016-06-24 18:05:1
	Q PME_OLD_00000a.	+	18류	9		F:\AhnLab\Product\	2016-04-20 17:41:52	2016-06-24 16:37:2
	Q PME_1_5.txt	+	16류	9		F:\AhnLab\Product\	2016-04-20 17:41:52	2016-06-24 16:37:2
	O PME_1_4_00000a.	+	18#	9		F:\AhnLab\Product\	2016-04-20 17:41:52	2016-06-24 16:37:1
	OPME_1_2_00000a.	. 1	1종류	9		F:\AhnLab\Product\	2016-04-20 17:41:52	2016-06-24 16:37:1
	O PME_1_1_00000a.	. +	16류	9		F:\AhnLab\Product\	2016-04-20 17:41:52	2016-06-24 16:37:1
	🧕 aaaa.txt	+	200月	10		F:\AhnLab\Product\	2016-04-20 17:41:16	2016-06-24 16:35:2
	PME_OLD_00000a.	+	18幕	9		F:\AhnLab\Product\	2015-12-14 18:19:05	2016-06-24 16:08:0
	PME_1_5.txt	1	16류	9		F:\AhnLab\Product\	2015-12-14 18:19:04	2016-06-24 16:08:0
	PME_1_4_00000a.	+	1종류	9		F:\AhnLab\Product\	2015-12-14 18:19:04	2016-06-24 16:08:0
	PME_1_2_00000a.	. +	18#	9		F:\AhnLab\Product\	2015-12-14 18:19:04	2016-06-24 16:08:0
	PME_1_1_00000a.	. 1	18幕	9	-	F:\AhnLab\Product\	2015-12-14 18:19:04	2016-06-24 16:08:0
	OLD_00000a.	+	1중류	9		F:\AhnLab\Product\	2016-02-23 16:53:49	2016-06-24 15:39:4
	PME_1_5.txt	+	18#	9		F:#AhnLab#Product#	2016-02-23 16:53:49	2016-06-24 15:39:4
	PME_1_4_00000a.	· 1	184	9		F:\AhnLab\Product\	2016-02-23 16:53:49	2016-06-24 15:39:3
	PME_1_2_00000a.	. +	16异	9		F:\AhnLab\Product\	2016-02-23 16:53:49	2016-06-24 15:39:3
	A DME 1 1 00000-		1122	0	1	ErWAhnt shittineduretit	2016 02 22 16:52:40	2016 06 24 15 20 2

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: PC에 소프트웨어 저작권 점검 프로그램이 한 번도 실행되지 않았거나, 관리자가 지정한 점검 날짜를 경과하였습니다. 프로그램 실행하기를 눌러 소프트웨어 저작권 점검을 수행하십시오.

점검 항목 상세 정보		
점검 결과: 취약	^	프로그램 실행하기
PC에 소프트웨어 저작권 점검 프로그램이 실행되지 않았습니다. ▶ [프로그램 실행하기]를 눌러 소프트웨어 저작권 점검을 수행하십시오.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

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

[프로그램 실행하기]

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

🧝 저작권 점검 - AhnLab Policy Agent 📃 💷 💌						
저작권 점검은, 한국 설치를 방지함으로/	점검 시작					
총 이 최근 점검이	저장하기 인쇄하기					
유형 저작권	사 소프트웨어 이름	제품 시리얼	설치일	최종 실행 파일		

●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.

점검 항목 상세 정보					
점검 결과: 취약	*	취약점 해결하기			
사용자 정의 점검 항목의 상태가 안전 조건과 일치하지 않습니다. ▶ 다음 안전 조건을 준수하며, 취약 항목에 대한 조치를 취하십시오.					
[Server 서비스 중지 점검] 설명 : 파일, 인쇄 및 명명된 파미프를 네트워크를 통해 공유할 수 있도록 지원합니다.					
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.					
	Ŧ	<u>조치 방법 상세 안내</u>			

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 해결하기를 통해 서비스 상태를 변경할 수 있습니다.

- 1. 점검 항목 상세 정보에서 취약점 해결하기를 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 조건을 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 해제하기를 눌러 모든 전체 공유 폴더를 해제하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	곳으 폭더 해제하기
PC에 1개의 전체 공유로 쓰이는 공유 폴더가 있습니다 ▶ [공유 폴더 해제하기]를 눌러 모든 사용자 공유 폴더를 해제하십시오.		
새 폴더		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

점검 결과가 취약인 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 해제하기를 누릅니다.
- 2. 공유 폴더 목록이 표시됩니다.

사용자 공유 폴더 보기 -	AhnLab 내PC지키미		×
공유 폴더 이름 temp3	볼더 경로 F:₩temp3		공유 폴더 해제
공유 폴더 설명			
		<u> </u>	모든 공유 폴더 해제
			닫기

- 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 해제를 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. 설정하기를 눌러 하드디스크 파일 시스템이 NTFS 를 사용하도록 설정하십시오.

점검 항목 상세 정보		
점검 결과: 취약	^	워클릭 조치
PC에 하드디스크의 파일 시스템이 NTFS를 사용하도록 설정되어 있지 않습니다. ▶ [원클릭 조치]를 눌러 하드디스크 파일 시스템이 NTFS를 사용하도록 설정하십시오.		
C: - NTFS 사용 D: - NTFS 사용 G: - NTFS 미사용 F: - NTFS 사용		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍니다.	Ŧ	<u>조치 방법 상세 안내</u>

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 조치를 누릅니다.
- 2. 원클릭 조치를 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.

C:#Windows#system32#convert.exe		x
파일 시스템 유형은 FAT32입니다. G: 드라이브의 볼륨 레이블을 입력하십시오. 새 볼륨		4 III

3. 알림 창에서 확인을 누르면 점검 결과는 안전으로 변경됩니다.

[사용자 조치]

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

- 1. 점검 항목 상세 정보에서 현재 PC의 하드디스크 파일 시스템의 NTFS 사용 현황을 파악합니다.
- 2. 시작 > 실행을 클릭하여, cmd를 입력한 다음 확인을 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.

한참고

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 조치를 눌러 NTP 시간 서버와 자동 동기화를 설정하십시오.

점검 항목 상세 정보	
점검 결과: 취약	· 원클릭 조치
PC에 NTP 시간 서버와 자동 동기화가 설정되어 있지 않습니다. ▶ [원클릭 조치]를 눌러 NTP 시간 서버와 자동 동기화를 설정하십시오.	
PC에 NTP 시간 서버와 자동 동기화가 설정되어 있습니다.	
	조치 방법 상세 안내
	-

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 조치를 누릅니다.
- 2. NTP 시간 서버와 자동 동기화가 설정하면 다음과 같은 알림 창이 나타납니다.

AhnLab LHPC	גו≠ום	×
i	NTP 시간 서버와 자동 동기화를 설정되었습니다.	
	확인	

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.cpl를 입력합니다.

💷 실행		<u> </u>
	프로그램, 폴더, 문서 또는 (인터넷 주소를 입력하십시오.
열기(<u>O</u>):	timedate.cpl	•
	🚱 이 작업은 관리자 권한	으로 실행됩니다.
	확인	취소 찾아보기(B)

2. 우측 상단의 인터넷 시간 탭을 클릭합니다.

📷 날짜 및 시간	×
날짜 및 시간 추가 시계 인터넷 시간	
날짜: 2015년 7월 22일 수요일 시간: 오전 9:51:18	
표준 시간대 (UTC+09:00) 서욱	
표준 시간대 변경(Z) 이 표준 시간대에서는 일광 절약 시간을 사용하지 않습니다.	
<u>표준 시간대에 대한 추가 정보를 온라인에서 가져오기</u> 시계 및 표준 시간대 설정 방법	
확인 취소 적용(A)

3. **설정 변경**을 클릭합니다.

📸 날짜 및 시간
날짜 및 시간 추가 시계 인터넷 시간
이 컴퓨터가 'time.windows.com'과(와) 자동으로 동기화되도록 설정되었습 니다.
이 컴퓨터는 예약된 일정에 따라 자동으로 동기화되도록 설정되어 있습니 다.
중 설정 변경(C)
인터넷 시간 동기회란?
확인 취소 적용(A)

 인터넷 시간 서버와 동기화를 체크 후 서버에 time.windows.com 또는 조직 내 지정된 NTP 시간 서버의 주소를 입력한 후 확인을 클릭하여 설정을 종료합니다.

📸 날짜 및 시간
날짜 및 시간 추가 시계 인터넷 시간
이 컴퓨터가 'time.windows.com'과(와) 자동으로 동기화되도록 설정되었습 니다.
💼 인터넷 시간 설정 📃 🏹
인터넷 시간 설정 구성:
☑ 인터넷 시간 서버와 동기화(S) 서버(E): time.windows.com ▼ 지금 업데이트(U)
이 컴퓨터는 예약된 일정에 따라 자동으로 동기화되도록 설정되어 있습니 다.
확인 취소
인터넷 시간 동기화란?
확인 취소 적용(A)

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 설치하기를 눌러 최신 버전의 보안 업데이트를 설치하십시오.

점검 항목 상세 정보		
점검 결과: 취약	*	업데이트 설치하기
Adobe Air (x86)가 최신 업데이트 상태가 아닙니다. (현재 버전: 21,0,0,176) ▶ 최신 버전인 21,0,0,179로 업데이트하시기 바랍니다.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하여 PC의 안정성을 최종 점검하시기 바랍 니다.		
		<u>조치 방법 상세 안내</u>

조치 방법

점검 결과가 **취약**일 때, <u>APM 라이선스가 없는 경우</u>와 <u>APM 라이선스가 있는 경우</u>에 따라 다음과 같이 조치하여 주시기 바랍니다.

[APM 라이선스가 없는 경우]

- 1. 점검 항목 상세 정보에서 업데이트 설치하기를 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.

점검 항목 상세 정보		
점검 결과: 취약	*	업데이트 설치하기
Adobe Air (x86)가 최신 업데이트 상태가 아닙니다. (현재 버전: 21,0,0,176) ▶ 최신 버전인 21,0,0,179로 업데이트하시기 바랍니다.		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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

25	보기 🔹 1개	비선택			› 적용된 패치 목록 (
	패치 분류	위호	비도	패치 변호	패치 이름
	일반 SW 패치		긴급	MS15-057	Windows Media Player의 취약성으로 인한 원격 코드 실행 문
~	일반 SW 패치	111	중요	Adobe AIR	Adobe AIR Update (22.0.0.153)
	일반 SW 패치	1111	긴급	MS12-016	.NET Framework 및 Microsoft Silverlight의 취약점으로 인한
	일반 SW 패치		긴급	MS12-025	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
	일반 SW 패치	1111	긴급	MS12-035	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
	일반 SW 패치		긴급	MS12-038	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
	일반 SW 패치		긴급	MS12-045	Microsoft Data Access Components의 취약점으로 인한 원격
	일반 SW 패치	1111	긴급	HNC 2010	HNC 2010 업데이트 (000858)
	일반 SW 패치		긴급	MS-KB2820331	Windows 7 및 Windows Server 2008 r 2에 대 한 응용 프로
	일반 SW 패치		긴급	MS-KB2786081	로그 오프하거나 Windows 7 SP1 또는 Windows Server 200
	일반 SW 패치		긴급	MS-KB2552343	Windows 7 또는 Windows Server 2008 R2가 실행되는 컴퓨
	일반 SW 패치		긴급	MS-KB2813430	An update is available that enables administrators to update
	일반 SW 패치		긴급	MS13-053	Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드
	일반 SW 패치	100	긴급	MS13-057	Windows Media Format Runtime의 취약점으로 인한 원격 코
	일반 SW 패치		중요	MS13-058	Windows Defender의 취약점으로 인한 권한 상승 문제점 (28
	일반 SW 패치	ш	중요	JAVA SE Runtime Envir	JAVA SE Runtime Environment 8 (008092)
	일반 SW 패치		긴급	Adobe Flash Player 14	Security updates available for Adobe Flash Player(APSB14-18)

3. 지금 업데이트를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.

4. 패치 적용이 완료되면 화면 상단의 적용된 패치 목록을 눌러 설치된 패치 정보를 확인할 수 있습니다.

위형	철도	패치 변호	패치 이름	패치 발표일	패치 설치 날짜
	중요	MS15-060	Microsoft 공용 컨트롤의 취약성으로 인한 원격	2015/06/09	
	긴급	MS15-067	RDP의 취약성으로 인한 원격 코드 실행 문제(3	2015/07/14	
	중요	Adobe AIR	Adobe AIR Update (22.0.0.153)	2016/06/16	2016/06/21
	긴급	Adobe Rea	Security updates for Adobe Reader and Acrob	2015/10/13	2016/06/21
	긴급	MS-KB2533	Windows 7 SP1, Windows Server 2008 R2 SP	2013/06/03	
	긴급	MS-KB2861	Microsoft 보안 공지: 원격 데스크톱 프로토콜	2013/08/13	
	긴급	MS13-083	Windows 공용 컨트롤 라이브러리의 취약점으	2013/10/09	
III	중요	MS-KB2731	Windows 7 또는 Windows Server 현지 시간과	2012/10/08	
	중요	MS15-030	원격 데스크톱 프로토콜의 취약점으로 인한 서	2015/03/10	
		기업도 ····································	비정 인호 비정 인호 비 중요 MS15-060 비 경요 MS15-067 비 경요 Adobe AIR 비 긴급 Adobe AIR 비 긴급 MS-KB2533 비 긴급 MS-KB2533 비 긴급 MS-KB261 비 긴급 MS-KB261 비 길급 MS13-083 비 중요 MS-KB2731 비 중요 MS15-030	취업도 배시 민호도 배시 민호도 배시 민호도 III 중요 MS15-060 Microsoft 공용 컨트롤의 취약성으로 인한 원격 III 긴급 MS15-067 RDP의 취약성으로 인한 원격 코드 실행 문제(3 III 긴급 Adobe AIR Adobe AIR Update (22.0.0.153) III 긴급 Adobe Rea Security updates for Adobe Reader and Acrob III 긴급 MS-KB2533 Windows 7 SP1, Windows Server 2008 R2 SP III 긴급 MS-KB2861 Microsoft 보안 공지: 원격 데스크톱 프로토를 III 긴급 MS13-083 Windows 7 또는 Windows Server 현지 시간과 III 중요 MS15-030 원격 데스크톱 프로토를의 취약점으로 인한 서	취업도 폐지 민료도 폐지 말료들 III 중요 MS15-060 Microsoft 공용 컨트롤의 취약성으로 인한 원격 2015/06/09 III 건글 MS15-067 RDP의 취약성으로 인한 원격 코드 실행 문제(3 2015/07/14 III 중요 Adobe AIR Adobe AIR Update (22.0.0.153) 2016/06/16 III 건글 Adobe Rea Security updates for Adobe Reader and Acrob 2015/10/13 III 건글 MS-KB2533 Windows 7 SP1, Windows Server 2008 R2 SP 2013/06/03 III 건글 MS-KB2861 Microsoft 보안 공지: 원격 데스크톱 프로토를 2013/08/13 III 건글 MS13-083 Windows 7 또는 Windows Server 현지 시간과 2012/10/08 III 중요 MS15-030 원격 데스크톱 프로토를의 취약점으로 인한 서 2015/03/10

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 설치하기를 눌러 최신 버전의 보안 업데이트를 설치하십시오.

점겸 항목 상세 정보		
점검 결과: 취약	*	업데이트 설치하기
Java SE Runtime Environment가 최신 업데이트 상태가 아닙니다. ▶ 최신 버전으로 업데이트하시기 바랍니다.		
Java Runtime Environment 8 현재 버전: 8,0,920,14 -> 최신 버전: 9,0,770,3		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

조치 방법

점검 결과가 **취약**일 때, <u>APM 라이선스가 없는 경우</u>와 <u>APM 라이선스가 있는 경우</u>에 따라 다음과 같이 조치하여 주시기 바랍니다.

[APM 라이선스가 없는 경우]

- 1. 점검 항목 상세 정보에서 업데이트 설치하기를 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.

점검 항목 상세 정보		
점겸 결과: 취약	^	업데이트 설치하기
Java SE Runtime Environment가 최신 업데이트 상태가 아닙니다. ▶ 최신 버젼으로 업데이트하시기 바랍니다.		
Java Runtime Environment 8 현재 버젼: 8,0,920,14 -> 최신 버젼: 9,0,770,3		
* 위 취약 항목에 대한 후속 조치 후, 보안 점검을 한번 더 수행하며 PC의 안정성을 최종 점검하시기 바랍 니다.		
	Ŧ	<u>조치 방법 상세 안내</u>

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

2두	보기 💌 1개	선택			* <u>적용된 패치 목록</u> 🕻
	패치 분류	위험	범도	패치 변호	패치 이름
	일반 SW 패치	IIII	긴급	MS15-057	Windows Media Player의 취약성으로 인한 원격 코드 실행 문
	일반 SW 패치		긴급	MS12-016	.NET Framework 및 Microsoft Silverlight의 취약점으로 인한
	일반 SW 패치		긴급	MS12-025	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
	일반 SW 패치		긴급	MS12-035	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
	일반 SW 패치		긴급	MS12-038	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점 (
	일반 SW 패치	HH	긴급	MS12-045	Microsoft Data Access Components의 취약점으로 인한 원격
	일반 SW 패치		긴급	HNC 2010	HNC 2010 업데이트 (000858)
	일반 SW 패치	1111	긴급	MS-KB2820331	Windows 7 및 Windows Server 2008 r 2에 대 한 응용 프로
	일반 SW 패치	1111	긴급	MS-KB2786081	로그 오프하거나 Windows 7 SP1 또는 Windows Server 200
	일반 SW 패치		긴급	MS-KB2552343	Windows 7 또는 Windows Server 2008 R2가 실행되는 컴퓨
	일반 SW 패치		긴급	MS-KB2813430	An update is available that enables administrators to update
	일반 SW 패치		긴급	MS13-053	Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드
	일반 SW 패치	1111	긴급	MS13-057	Windows Media Format Runtime의 취약점으로 인한 원격 코
	일반 SW 패치	m	중요	MS13-058	Windows Defender의 취약점으로 인한 권한 상승 문제점 (28
~	일반 SW 패치	ш	중요	JAVA SE Runtime Envir	JAVA SE Runtime Environment 8 (008092)
	일반 SW 패치	1111	긴급	Adobe Flash Player 14	Security updates available for Adobe Flash Player(APSB14-18)

3. 지금 업데이트를 눌러 적용되지 않은 패치 목록을 업데이트 합니다.

4. 패치 적용이 완료되면 화면 상단의 적용된 패치 목록을 눌러 설치된 패치 정보를 확인할 수 있습니다.

배치 분류	위형	법도	패치 변호	패치 이름	패치 발표일	패치 설치 날짜
운영 체제 패치	ш	중요	MS15-060	Microsoft 공용 컨트롤의 취약성으로 인한 원격	2015/06/09	
운영 체제 패치	1111	긴급	MS15-067	RDP의 취약성으로 인한 원격 코드 실행 문제(3	2015/07/14	
일반 SW 패치		중요	Adobe	Adobe AIR Update (22.0.0.153)	2016/06/16	2016/06/21
일반 SW 패치	100	긴급	Adobe	Security updates for Adobe Reader and Acrob	2015/10/13	2016/06/21
일반 SW 패치	100	긴급	MS-KB2	Windows 7 SP1, Windows Server 2008 R2 SP	2013/06/03	
운영 체제 패치		긴급	MS-KB2	Microsoft 보안 공지: 원격 데스크톱 프로토콜	2013/08/13	
운영 체제 패치	1111	긴급	MS13-083	Windows 공용 컨트롤 라이브러리의 취약점으	2013/10/09	
일반 SW 패치	111	중요	JAVA S	JAVA SE Runtime Environment 8 (008092)	2016/04/20	2016/06/21
운영 체제 패치	111	중요	MS-KB2	Windows 7 또는 Windows Server 현지 시간과	2012/10/08	
운영 체제 패치	111	중요	MS15-030	원격 데스크톱 프로토콜의 취약점으로 인한 서	2015/03/10	

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 조치를 눌러 허용되지 않은 IP 주소를 사용하지 않도록 설정하십시오.

점검 항목 상세 정보		
점경 결과: 취약	^	원클릭 조치
▶ [원클릭 조치]를 눌러 허용되지 않은 IP 주소를 사용하지 않도록 설정하십시오.		
172, 16, 88, 114 abodisk 172, 16, 11, 158 master		
		<u>조치 방법 상세 안내</u>
	-	

조치 방법

조치 방법에는 원클릭 조치 버튼을 통해 조치할 수 있습니다.

[원클릭 조치]

- 1. 점검 항목 상세 정보에서 원클릭 조치를 누릅니다.
- 2. 허용되지 않은 IP 주소를 사용하지 않도록 설정하면 다음과 같은 알림 창이 나타납니다.
- 3. 알림 창에서 확인을 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 안내를 참고하여 허용되지 않은 DNS 서버 주소를 사용하지 않도록 설정하십시오.

^	
	<u>조치 방법 상세 안내</u>
	*

조치 방법

점검 결과가 취약인 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 센터로 이동합니다.
- 2. <네트워크 및 공유 센터>에서 어댑터 설정 변경을 누릅니다.



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

					x
중 ♥ 😨 > 제어판 > 네트워크 및 인터넷 > 네	트워크	크 연결 ▶	↔ 네트워크 연결 검색	_	P
구성 ▼ 이 네트워크 장치 사용 안 함 이 연결	진단	이 연결 이름 바꾸기	이 연결의 상태 보기 🛛 🕷	N .	?
TrusZone VMware VMware VTN Network Network			1		
Adapter Adapter VMnet1 VMnet8	V	사용 안 함(B) 상태(U) 진단(I)			
	۲	연결 브리지(G)			
	(i) (i)	바로 가기 만들기(S) 삭제(D) 이름 바꾸기(M)			
	0	속성(R)			

4. <로컬 영역 연결 속성>의 네트워킹 탭에서 Internet Protocol Version 4(TCP/IPv4)를 선택하고, **속성**을 누릅니다.

📮 로컬 영역 연결 속성 📃 🎽 💌
네트워킹 공유
연결에 사용할 장치:
Intel(R) Ethernet Connection (2) I218-V
이 연결에 다음 항목 사용(0): 구성(C)
▼ ■ QoS 패킷 스케줄러 ▲ ▼ ■ Microsoft 네트워크용 파일 및 프린터 공유 ▲ ▼ ▲ Internet Protocol Version 6 (TCP/IPv6) ▲ ▼ ▲ Internet Protocol Version 4 (TCP/IPv4) ■ ▼ ▲ Link-Layer Topology Discovery Mapper I/O Driver ■ ▼ ▲ Link-Layer Topology Discovery Responder ▼
설치(N) 제거(U) 속성(R)
설명 전송 컨트롤 프로토콜/인터넷 프로토콜, 기본적인 광역 네트워 크 프로토콜로, 다양하게 연결된 네트워크에서 통신을 제공합니 다.
확인 취소

5. <Internet Protocol Version 4(TCP/IPv4) 속성>에서 기본 설정 DNS 서버와 보조 DNS 서버의 IP 를 확인합니다.

Internet Protocol Version 4 (TCP/IPv4) 속성	?
일반 대체 구성	
네트워크가 IP 자동 설정 기능을 지원히 할 수 있습니다. 지원하지 않으면, 네트 을 문의해야 합니다.	I면 IP 설정이 자동으로 할당되도록 워크 관리자에게 적절한 IP 설정값
◎ 자동으로 IP 주소 받기(0)	
● 다음 IP 주소 사용(S):	
IP 주조(I):	· · · · ·
서브넷 마스크(U):	
기본 게이트웨이(D):	
○ 자동으로 DNS 서버 주소 받기(B) _ ● 다음 DNS 서버 주소 사용(E):	
기본 설정 DNS 서버(P):	THE REPORT
보조 DNS 서버(A):	
🔲 끝벌 때 설정 유효성 검사(L)	고급(V)
	확인 취소

• 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 관리를 눌러 이름을 변경할 수 있습니다.

점검 항목 상세 정보	
점검 결과: 취약	▲ 프로세스 관리
최근 30일간 허용되지 않은 프로세스의 파일 접근을 탐지했습니다. (프로세스 개수: 1개)	
탐지 횟수 : 4 경로 : C:\Program Files (x86)\Notepad++\notepad++.exe	E
업무용 프로그램은 문서 보호 정책의 예외 정책으로 등록되도록 관리자에게 요청하십시오. 알 수 없는 프로세스는 [프로세스 관리]를 눌러 미름을 변경할 수 있습니다.	
	<u>조치 방법 상세 안내</u> ▼

조치 방법

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

[프로세스 관리]

1. 점검 항목 상세 정보에서 프로세스 관리를 누릅니다.

R	3 = 5	네스 관리	42	successful from the party of the	×
	지지마 *	- 30일 동안 허용되지 않은 프로 2용 프로그램은 문서 보호 정책 수 없는 프로세스는 [프로세스 [:세스가 파일에 접근 의 예외 정책으로 등 비름 변경]을 누르면	라는 것을 탐지했습니다(프로세스 개수: 1개, 접근 탐지 횟수: 3 록되도록 관리자에게 요청하십시오. , '프로세스 이름.exe_ahnlab'로 변경됩니다. (예: abc.exe_ahnlab)	회)
L	1개	선택			<u>변경 완료 목록</u>
	V	프로세스 이름	접근 탐지 횟수	프로세스 경로	
	V	notepad++.exe	3	C:\Program Files (x86)\Notepad++\notepad++.exe	
				프로세스 이름 변경	취소

- 2. <프로세스 관리>에서 변경을 원하는 프로세스를 선택한 뒤, 프로세스 이름 변경을 누릅니다.
- 3. 프로세스 이름 변경이 완료되면 다음과 같은 알림 창이 발생합니다.

AhnLab ЩPC⊼ ヲ □	— X —
(1) 허용되지 않은 프로세스의 (변경 프로세스: 1개	미름을 변경되었습니다.
확인	!

4. 확인을 누르면 점검 결과는 안전으로 변경됩니다.

9장

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.

한참고

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(之)에서 마우스 오른쪽을 눌러 사용자 정보를 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.

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 보기를 선택합니다.
- <공지사항>이 나타나면 내용을 확인합니다. 공지사항의 윗부분은 관리자가 보낸 공지사항 목록이며, 아래 부분은 목록에서 선택한 공지사항의 내용이 보입니다.

🍤 공지사항				- 0	23
제목	۸	간	7	작성자	1
	공지 사항 목록 표시 영역				
작성자 : 시간 : 제목 :					
	공지 사항 내용 표시 영역				

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(之)에서 마우스 오른쪽을 눌러 기타 옵션 > 고급 설정을 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 2개 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(之)에서 마우스 오른쪽을 눌러 제품 정보를 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.

한참고

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 이상 인지 확인합니다.

😻 Windows 보안 센터		
	사용자의 PC를 안전하게 !	😍 보안 센터 보호하도록 도와줍니다.
리소스 ※ • Microsoft에서 보안 및 바이러 스에 대한 최신 정보 받기 • Wedews Update에 내 취심 역	보안 설정 보안 센터는 Windows 보안 설정의 관리를 도와줍니다. 사용7 기 위해 다음세 가지의 보안 기능을 사용하도록 설정했는지 3 되어 있지 않은 경우 [권장 사항]을 따르십시오. 나중에 보안 을 여십시오. Windows에서 컴퓨터를 안전하게 보호하는 새로운 방법	따의 컴퓨터를 안전하게 보호하 확인하십시오, 사용하도록 설정 센터로 되돌마오려면 [제대판]
데이트 검색	😂 방화벽	사용 중 🛞
• 보안 센터에 관련된 도움말	🦥 자동 업데이트	설정 확인 🛛 😻
 보안 센터에서 사용자에게 알 림을 보내는 방법을 변경 	😺 바이러스 백신	사용 중 🛞
	바이러스 백신 소프트웨어가 최신으로 유지되어 있으며 바이 있음이 검색되었습니다. 바이러스 백신 소프트웨어는 사용 다른 보안 위험으로부터 보다 안전하게 보호합니다. 바이러스 백신 소프트웨어 및 컴퓨터 보안에 대한 자세한 정 사용 중인 바이러스 백신 소프트웨어: V3 Internet Security	기러스 경사 기능이 사용되고 자의 컴퓨터를 바이러스 및 <u>영보</u>
	보안 설정 관리 대상:	
	🚱 인터넷 옵션 🛛 🎯 Windows 방화벽	l.
	🐌 자동 업데이트	
Microsoft는 11.8.TI이 레이 저희를 난 추측	이디 시호자초 후체 수납 다 이 / 이 / 기 에	

- 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 > 실행을 누른 후 입력 창에 cmd를 입력합니다.

실행	
	프로그램, 폴더, 문서, 또는 인터넷 리소스 이름을 입력하십시오.
열기(<u>0</u>):	ems 💌
	확인 취소 찾아보기(용)

 명령어 창에 net stop winnight를 입력합니다. ***서비스를 멈추면 다음 서비스도 멈추어집니다. 이 작 업을 계속 하시겠습니까? 라는 메시지에 Y를 입력합니다.



- c:\windows\system32\wbem 폴더로 이동합니다. Repository 폴더의 이름을 다른 이름으로 변경 합니다.
 (예) Repository_abc
- 4. 명령어 창에 net start winmgmt를 입력합니다.



5. 명령어 창에 net start wscsvc를 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.

한참고

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.

한참고

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.

😻 Windows 보안 센터		
	사용자의 PC를 안전하게 5	
 이 리소스 Nicrosoft에서 보안 및 바이러 스에 대한 최신 정보 받기 Windows Update에 내 치신 약 	보안 설정 보안센터는 Windows 보안 설정의 관리를 도와줍니다. 사용자 기 위해 다음 세 가지의 보안 기능을 사용하도록 설정했는지 혹 되어 있지 않은 경우 [권장 사항]을 따르십시오. 나중에 보안 (을 여십시오. Windows에서 컴퓨터를 안전하게 보호하는 새로운 방법	1의 컴퓨터를 안전하게 보호하 1인하십시오. 사용하도록 설정 센터로 되돌아오려면 [제어판]
데이트 검색	😂 방화벽	사용 중 🛞
• 보안 센터에 관련된 도움말	🐌 자동 업데이트	설정 확인 😒
 보안 센터에서 사용자에게 알 림을 보내는 방법을 변경 	💋 바이러스 백신	사용 중 🌸
	바이러스 백신 소프트웨어가 최신으로 유지되어 있으며 바이 있음이 검색되었습니다. 바이러스 백신 소프트웨어는 사용기 다른 보안 위험으로부터 보다 안전하게 보호합니다. 바이러스 백신 소프트웨어 및 컴퓨터 보안에 대한 자세한 정	러스 검사 기능이 사용되고 ^{밖의} 컴퓨터를 바이러스 및 보
	사용 중인 바이러스 백신 소프트웨어: V3 Internet Security	
	보안 설정 관리 대상:	
	🚱 인터넷 옵션 🛛 🎯 Windows 방화벽	
	🐴 자동 업데이트	
Microsoft는 사용자의 개인 정보를 보호할	입니다. 개인 정보 보호 정책을 참조하십시오.	

- 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 > 실행을 누른 후 입력 창에 cmd를 입력합니다.

실행	28
	프로그램, 폴더, 문서, 또는 인터넷 리소스 미름을 입력하십시오.
열기(<u>0</u>):	ems
	확인 취소 찾아보기(<u>B</u>)

 명령어 창에 net stop winnight를 입력합니다. ***서비스를 멈추면 다음 서비스도 멈추어집니다. 이 작 업을 계속 하시겠습니까? 라는 메시지에 Y를 입력합니다.



- c:\windows\system32\wbem 폴더로 이동합니다. Repository 폴더의 이름을 다른 이름으로 변경 합니다.
 (예) Repository_abc
- 4. 명령어 창에 net start winmgmt를 입력합니다.



5. 명령어 창에 net start wscsvc를 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.

한참고

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.

- 🔋 Windows 보안 센터 🜒 보안 센터 사용자의 PC를 안전하게 보호하도록 도와칩니다 리소스 \$ 년]를 도와줍니다. 사용자의 컴퓨터를 안전하게 보 2를 사용하도록 설정했는지 확인하십시오. 사용하 사업)을 따르십시오. 나용에 보안 센터로 되겠다요 Microsoft에서 보안 및 바이러 스에 대한 최신 정보 방기 이십시오. 컴퓨터를 안전하게 보호하는 새로운 방법 Windows Update에서 최신 업 데이트 검색 사용안함 * 방화벽 • 보안에 관련된 지왕 받기 ndows에서 이 접류터에 하나 이상의 벽을 사용하도록 설정되어 있지 않습니 사항]을 클릭하십시오. 방화벽 및 걸 방화벽이 설치되어 있는 것을 감지했으나 방 니다. 이 문제를 해결하는 방법을 보려면 [권 프리 보이에 대한 지배하 정보 • 보안 센터에 관련된 도용말 보안 센터에서 사용자에게 알 링을 보내는 방법을 변경 권장 사항(B)... 🏷 자동 업데이트 사용중 * 🕗 바이러스 백신 사용안함 🔹 같이, 컴퓨터에서, 여러 렇씕힘짓임 사용하 년 분들 분들이 있습니다. 지 특히 실시오, 바이러스 백선 있음: 참고: Windows에서 모든 바이러스 혁신 프로그램을 감지하지는 권장 사항(E). 보안 성정 관리 대상: 🛃 인터넷 옵션 Windows 방화벽 Microsoft는 사용자의 개인 정보를 보호합니다. <u>개인 정보 보호 정책</u>을 참조
- 1. 시작 > 제어판에서 보안 센터를 실행합니다.
- 2. 보안 센터에서 바이러스 백신 영역에서 권장 사항을 선택합니다.

3. <권장 사항>에서 직접 관리하는 바이러스 백신 프로그램을 사용하고 있습니다. 를 선택 해제 합니다.



보안 센터 서비스 실행 여부

제어판에 보안 센터가 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.

+ + 📧 🖆 🕯								
🍫 서비스(로컬)	💫 서비스(루컬)							
	Security Center	018 /	설명	상태	시작 유	성 다음 사	8자로 로그온	0
	서비스 <u>시작</u>	Semiconter Registry Removable Storage Routing and Remote Access	원격 사용자 LANOILE WA	시작될	자동 수동 사용 안	로열 시 로컬 시 함 로컬 시	비스 스템 스템	
	설명: 시스템 보아 성정과 그성을 다니더하	Secondary Logon	다른 자격 중 공격 사용자	시작됨 시작되	자동	로벌 시 같법 1	스템 스템	
		Security Center	시스템 보안		XF9	2월 1	EAG 1	
	protection of the second se	Server .	이 컴퓨터에	시작된	714	적(요)		
		Shell Hardware Detection	자동 재생 하	시작팀	재	N(Q)	1	
		Smart Card	컴퓨터에서		41 ^S	(시 중지(U)	4	
		Smart TimeLock Service	Smart TimeL	시작됨	74 7	(A(M)	10	
		SSDP Discovery Service	홉 네트워크	시작됨	41 C	네 시작(E)	¥_	
		System Event Notification	Windows 星	시작될	재	E 7509/61	18	
		System Restore Service	시스템 복원	시작됨	재	E ARIDI	1	
		Task Scheduler	사용자가 켭	시작팀	재 씨	로 고침(E)	122	
		TCP/IP NetBIOS Helper	TCP/IPULA	시작될	74			
		Telephony Telephony	로컬 컴퓨터	시작됨	4! ⁴	(名(田)	10	
		Telnet	원격 사용자		사태 5	89:(H)	5	
		Terminal Services	원격 컴퓨터	시작됨	46-		ranks	
		Themes	사용자 경험	시작됨	자동	로벌 시	스챔	
		S TrusLine		시작됨	자동	로벌 시	스템	
		Supply Uninterruptible Power Supply	컴퓨터에 안		수동	로벌 시	비스	
		SUniversal Plug and Play Device Host	유니버설 플		수동	로벌 시	비스	
		Solume Shadow Copy	벽업과 기타		수동	受盟 시	스템	
		SwebClient	Windows 71	시작팀	政長	로벌 서	비스	
		S Windows Audio	Windows 71	시작될	자동	로벌 시	스 덤	
		Windows CardSpace	안견하게 티		수동	로벌 시	스템	
		SWindows Firewall/Internet Connection Shari	네트워크 주	시작됨	자동	로털 시	스템	
		Windows Image Acquisition (WIA)	스케너 및 카		수동	로벌 시	스템	
		S Windows Installer	Windows Ins		수동	로벌 시	스템	
		SWindows Management Instrumentation	운영 체제, 장	시작됨	자동	星間 人	스템	
		Sindows Management Instrumentation Drive,	5501H0		수동	로벌 시	스템	
		S Windows Presentation Foundation Font Cach	Optimizes p		수동	로벌 사	비스	×

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(<u>http://update.microsoft.com</u>)에 접속합니다.
- 2. 업데이트 화면에서 사용자 지정 설치를 선택합니다.

Microsoft [®]				
Microsoft Update				
Microsoft Update 홈	환양	영합니다 !		
	Micros	oft Update		
옵션				
업데이트 내역 검토				
숨겨진 업데이트 복원	금 규칙 을 적인 경제로 유지 Windows, 프로그램, 하드웨어 또는 장치에 업데이트가 필요한지 확인하십시오.			
설정 변경				
질문과 대답	빠른 설치	중요 업데이트 다운로드 (권장)		
도움말 및 지원 보기				
관리자 옵션 사용	사용자 지정 설치	Windows 및 다른 프로그램에 대한 선택적 업 데이트와 중요 업데이트 중에서 선택합니다.		
	개인 정보 보호 정책 업데이 사용됩니다. 사용자 개인 정보	I트를 검색하면 사용자의 프로그램에 필요한 업데이트를 본는 사용되지 않습니다. 자세한 내용을 보려면 개인 정보		

3. 지금 다운로드 및 설치를 누릅니다.

Microsoft	Microsoft.com에서 검색:	34
Microsoft Update		
Microsoft Update	Windows XP Service Pack 3	
🔁 업데이트 설치	컴퓨터 보호를 위해 Windows XP 서비스 팩 3를 설치하는 것이 좋습니다. 자세한 내용은 SP3의 새로운 기능(What's New in SP3)을 참 섭시오.	조하
읍년 업데이트 내역 경토 승거진 업데이트 북원 실정 변경 중문과 대답 도유만의 지원 법계	지금 다운로드 및 설치 • 기다리는 동안 다른 프로그램을 사용할 수 있습니다. 다운로드가 중단되는 경우 다음에 Microsoft Update에 연결하면 다운로드가 다시 시작됩니다. • 또한 자동 업데이트를 설정하여 자동으로 다운로드하거나 SP3를 CD로 주문할 수도 있습니다. • 설치 건에 알아 두어야 할 사항…	
고명을 및 시정 도기 관리자 옵션 사용	다운로드 크기: 0 KB, 0 분 (다운로드 완료 및 설치 가능) Windows XP 서비스 팩 (XSP3)은 Windows XP에 대한 고객의 주요 의견을 반영하여 업데이트된 Windows XP의 업데이트 버젼으 보안 업데이트 중 이건에 발표된 Windows XP용 업데이트가 모두 포함되어 있는 누적 업데이트입니다. Windows XP SP3에는 세료 업데이트가 일부 포함되어 있지만 Windows XP 환경을 크게 변경하지는 않습니다. 이 업데이트를 설치한 후 시스템을 다시 시작하여 합니다. <u>자세한 정보</u>	로,원 6
	기타 업데이트 캠토 및 설치 이 Windows XP 서비스 팩 3(KB936929)를(물) 설치하지 않으면 다 은 업데이트가 사용자의 컴퓨터에 계속 적용될 수 있습니다.	

4. <업데이트 설치>가 나타나면 설치를 원하지 않는 항목에 대해 동의 안 함을 선택합니다.

🌯 업데이트 설치
이 사용 약관 읽기(1/1) 업데이트를 설치하려면 사용 약관 내용에 동의해야 합니다. Windows XP 서비스 팩 3(KB936929)
MICROSOFT 소프트웨머에 대한 추가 최종 사용자 사용권 계약서 MICROSOFT WINDOWS XP 서비스 팩 3
본 추가 최종 사용자 사용권 계약서("추가 사용권 계약서")를 자세히 읽으시기 바랍니다. 본 추가 사 용권 계약서가 동봉된 소프트웨어를 설치 및 사용함 과 동시에 본 추가 사용권 계약서의 내용에 동의하 게 됩니다. 사용권 계약서 내용에 동의하지 않으면 소프트웨어를 설치하거나 사용하지 마시기 바랍니다
<u>인쇄 버전</u> 동의 안 함(<u>D</u>) 동의 함(<u>A</u>) 취소

5. <사용 약관에 동의 안 함>이 나타나면, 업데이트의 설치 여부를 다시 묻지 않습니다. 를 선택하고 확인을 누릅니다.

사용 약관에 동의 안 함 🛛 🔀
업데이트를 설치하지 않습니다.
✓업데이트의 설치 여부를 다시 묻지않습니다(D).
확인 취소

 <업데이트 설치>에서 업데이트 완료 후 일부 업데이트가 설치되지 않았습니다. 라는 메시지가 표시되고 설치되지 않은 항목을 보여줍니다.

🖏 업데이트 설치 🛛 🔁		
2	일부 업데이트가 설치되지 않았습니다. 모든 업데이트를 건너뛰도록 선택했으므로 사용자 컴퓨터에는 변경된 내용이 없습니다.	
	다음 업데이트가 설치되지 않았습니다.	
	Windows XP 서비스 팩 3(KB936929)	
자동 업데이트 구성		닫기

자동 업데이트())에서 업데이트 숨기기

- 1. 작업 표시줄의 자동 업데이트 ())을 선택합니다.
- 2. 사용자 정의 설치(고급)을 선택하고 다음을 누릅니다.
- <자동 업데이트>의 업데이트 제목에 표시된 항목 중 설치하지 않을 항목을 선택 해제하고 닫기를 누릅니다.

🐐 자동 업데이트	×
👌 설치할 업데이트 선택	
업데이트 제목	
자세히	
⊒7I: 69.5MB - 315.8MB	
Windows XP 서비스 팩 3(SP3)은 Windows XP에 대한 고객의 주요 의견을 반영하여 업데이트된 Windows XP의 업데이트 버전으로, 보안 업데이트 등 이전에 발표된 Windows XP용 업데이트가 모두 포함되어 있는 누적 업데이트입니다. Windows XP SP3에는 새로운 업데이트가 일부 포함되어 있지만 Windows XP 환경을 크게 변경하지는 않습니다. 이 업데이트를 설치한 후 시스템을 다시 시작해야 합니 다	
자동 업데이트 설정 변경 취소 취소	

4. <업데이트 숨기기>에서 업데이트를 다시 알리지 않습니다. 를 선택하고 확인을 누릅니다.

MS 홈페이지에서 업데이트 숨기기

- 1. MS 업데이트 사이트(<u>http://update.microsoft.com</u>)에 접속합니다.
- 업데이트 목록에서 설치를 원하지 않는 항목의 선택을 해제하고, 이 업데이트를 다시 표시 안 함을 선택합니다.


숨긴 업데이트 항목 표시

- 1. MS 업데이트 사이트(<u>http://update.microsoft.com</u>)에 접속합니다.
- 2. 업데이트 화면에서 업데이트 검토 및 설치를 누릅니다.
- 3. 중요 업데이트가 숨겨져 있습니다. 메시지 영역에서 지금 복원을 누릅니다.

📣 검색 결과 사용자 지정
업데이트 검토 및 설치
업데이트 설치 다운로드 크기(총): 0 KB 현재 연결 속도에서의 예상 시간: 0 분
중요 중요 업데이트가 숨겨져 있습니다. 하나 이상의 중요 업데이트를 숨기도록 지정했는데, 이 업데이트를 설치하기 전에는 컴퓨터가 안전하지 않을 수 있습니다. 지금 복원
중요 업데이트를 업데이트를 선택하지 않았습니다. 왼쪽의 옵션을 사용하며 사용 가능한 업데이트를 선택하십시오. 컴퓨터에 필요한 중요 업데이트를 모

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.

- 미사용 ActiveX 프로그램 존재 점검 항목에서 취약으로 진단된 경우 점검 항목 상세 정보 옆에 있는 ActiveX 삭제하기를 실행합니다.
- 미사용 ActiveX 프로그램 목록이 화면에 나타납니다. 목록에서 삭제할 대상을 선택한 후에 ActiveX 삭 제하기를 누릅니다.

2	ActiveX 프로그램 이름 COWebForKIPO Control	마지막 사용 날짜 2014-06-24 13:26:04	다운로드 주소 C:₩PROGRA~1₩EPS₩KTPO₩COWEBE~1.(OCX
	CQVVEDI GINLE'O CONCON	2014-00-24 13:20:04	Carrisonovi a crossico a concentro	Jen
			ActiveX 삭제하기	정보
١ <u>ت</u>	를 누르면 ActiveX 프로그램	목록에서 선택한 대상을	삭제합니다.	

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

2006	edForkipO Control	
	CLSID	CQWebForKIPO Control
	파일 절대 경로	{63A7967F-5300-48FC-984B-16FC0D69BD99}
	다운로드 받은 사이트	http://www.patent.go.kr/ocx/CQWebForKIPO.cab
	게시자	{86FD811E-44E2-47AB-94C4-6CCF853B9ED1}
	인증자	CQWebForKIPO
	마지막 사용일	2014-06-24 13:26:04
		·
		닫기

3. 삭제 진행 과정이 표시되며, 삭제가 완료되면 확인을 눌러 창을 닫습니다.

ActiveX 프로그램 삭제 - AhnLab 내PC지키미	
ActiveX 프로그램 삭제를 마쳤습니다. 100%	
확인	

한참고

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.

AhnLab LiiP	[지키]				0	• ×
HOME	PC 점겸	파스위드 점검 도구	PC 최적화	보고서		
			최근 점검	결과 2016	. 06, 01, 10:18 (결과 전송 완료)	
					49건	
				 9건		
		[근 PC 점검 점수	점검 불기	• 2건		
		85점	점겸 점수	추이	최근 1회	
			· 85점			
			06/01			
			10:18			
			PC 최적화	날자		
	• <u>PC 점검 점수</u> (<u> 반영 항목</u>			다음 점검일까지 남은 날짜: 14일	

한참고

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.
- C:\Program Files\AhnLab\APC2\MyPCInspector 폴더에 있는 MyPCUI.exe 에서 마우스 오른쪽을 누른 후 보내기 > 바탕 화면에 바로 가기 만들기를 선택합니다.

	Filer • Abol ab • ADC ²	A Mi@Clasactor	the state	- 4. 14.075	martor 244		×
구성 * 열기 년	토환성 파일 새 콜더	· MyPCInspector ·		• • • • • • • • • • • • • • • • • • •	li	• 🗄	
☆ 즐겨찾기 ▲ 다운로드 월 최근 위치 중 라이브러리 한 문서 월 비디오 ▲ 사진 한 음악 분 컴퓨터 출 로컬 디스크 (C:) 오 Shared(\\#10.2.2.3() ↓ 네트워크	OI를 MyPCSvc MyPCUI MyPCUI MyPCUD MyPCUD MyPCUp MyPCUp MyPCUp MyPCUp MyPCUp MyPCUp MyPCUp MyPCUp MyPCUp MyPCUp MyPCUp MyPCUP MPCUP MPCU	^ 수정한 2013-0 2014 V3 ZIPOS 202-0 203-0 V3 PC 234- V3 PC 234- V3 PC 244- V3	날짜 유 3-21 오후 응 3-21 오후 응 4.03 오전 응 유 위 유 유 유 유 유 유 유 유 유 유 유 유 유	명 용 프로그램 용 프로그램 용 프로그램 성 설정 용 프로그램 스토 문서 용 프로그램 확장 용 프로그램 확장 용 프로그램 확장 용 프로그램 확장 응 프로그램 확장 응 프로그램 확장 등 플로그램 확장 등 플로그램 확장 등 플로그램 확장 등 프로그램 확장	⊒7 1,252×8 832×8 2,253×8 1K8 364K8 433K8 13K8 13K8 32K8 104×8 36K8 40×8 56×8 80×8 140×8 80×8 140×8 80×8		
	PaLogU.DLL PaLogX64.D PaNetApi.dll PaRboot	국가(C) 바로 가기 만들기(S) 삭제(D) 이름 바꾸기(M)		팩스 수신자 편지 수신자 Shared(\#10.2.2.3	0) (Z:)		-
MyPCUI 석 응용 프로그램	2013- 크기: 2.19Mp	속성(R)	15				

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()이 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 시작을 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.

AhnLab Privacy Management(P)		
AhnLab 내PC지키미(T)	1	
AhnLab Patch Management(C)		
사용자 정보(I) 공지 사항 보기(V) 기타 옵션		•
제품 정보(A) 서버 연결 상태 확인		
끝내기(X)		

3. AhnLab 내PC지키미 메뉴를 누르면 메인 창이 나타납니다. 실행된 메인 창에서 내PC지키미 검사를 수 행할 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.

🛃 AhnLab Lii P	C지키미						(accord	• ×
HOME	PC 점검	피스위드 점검 도구	PC 최적화	보고서				
			최근 점겸	결과 2016	, 03, 30, 1	1:00 (결과 전:	응 완료)	
					- 112			
		\sim	위약 	■ 1건 • 7				
	2	I근 PC 점검 점수						
		90점	점경 점수	本미 			의근 5회 	
			<u>90점</u>					
							03/30 11:00	
			PC 최적화	날짜			비화 실행	
	• <u>PC 점검 점수</u> !	<u>반영 합목</u>			다음 점	겁일까지 남은	날짜: 7일	

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 수행 할 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.

P 로그인-AhnLab	MyPCInspector	×						
내PCス ヲ ロ Copyright (C) AhnLab, Inc. 2002-2014. All rights reserved.								
서버 선택 아이디 비밀번호	mypcadmin							
<u>옵션 =</u>		로그인						

2. 서버의 IP 가 잘못 입력되어 있는 경우 좌측 하단의 **옵션**을 클릭하여 IP 주소를 수정 후 재 로그 인을 시도 합니다.

P. E	그인 - AhnLab I	MyPCInspector	×
L G	 PC⊼ ₹ □ pyright (C) Ah	nLab, Inc. 2002-2014. All rights reserve	ed.
	서버 선택	부천 (250) *	
	아이디	mypcadmin	
	비밀번호		
	서버 이름	부전	
	₽ 주소	. 250	
	<u>76</u>	2002	
	ofold	mypcadmin	수정
	서비 목록		
	기본 서비		추가
	주전 수원1		삭제
	의정부 용인	17	
	연천		
	<u>선 •</u>	1	로그언

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.

P 로그인-Ahr	Lab MyPCInspector	×
내PC지키 Copyright (C	(0) C) AhnLab, Inc. 2002-2014. All rights reserved.	
서비 선택	부친 (250)	
010101	mypcadmin	
비일번호		
서버 이름	부전	
₽ 주소	. 250	
<u>⊒∈</u>	2002	
아이디	mypcadmin	수정
서비 목록		
기본 서비	۹.	추가
수원1		낙제
의성부 용인		
면천		
<u>옵션 *</u>		9.32

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(学)을 누르면, 사용자 정보를 에이전트 사용자가 직접 입력할 수 있습니다.

- 1. 작업 표시줄의 에이전트 아이콘(之)에서 마우스 오른쪽을 눌러 사용자 정보를 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.

1 2 m	ypcagentSetup.exe은(는) 일반적으로 다운로드되는 파일이 아니며, 컴퓨터를 손상 시킬 수 있습니다.	삭제(D)	작업(A)	다운로드 보기(V) ×
2. 다	·음 화면에서 좌측 하단의 기타 옵션 을 선택합니다.			
Smarts	Screen 필터 - Windows Internet Explorer			
8	이 프로그램은 컴퓨터를 손상시킬 수 있습니다. 계시자: 알 수 없음 이를: mypcagentSetup.exe SmartScreen 필터가 이 프로그램은 일반적으로 다운로드되는 파일이 아니 며 작성자의 서명이 포함되어 있지 않다고 보고했습니다. 이 프로그램을 예기지 않은 요정, 링크 또는 첨부 파일로 받은 경우 사용자 을 속이려는 시도일 수 있습니다. 이 프로그램을 삭제하는 것이 좋습니다.			
Smart	 → 이 프로그램 실행 안 함 → 프로그램 삭제 기타 옵션 Screen 필터란? 			

 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.



 최신 보안패치가 적용되어 있지 않은 경우 다음과 같은 화면이 보이며 업데이트 확인 버튼을 눌러 업 데이트를 실행합니다.



 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

PC 점검 21 PC 최적화 151 보 보고서 153

패

패스워드 점검 149

Ahnlab

경기도 성남시 분당구 판교역로 220 (우)13493 홈페이지: http://www.ahnlab.com 대표전화: 031-722-8000 팩스: 031-722-8901 © 2017 AhnLab, Inc. All rights reserved.