

Avira Internet Security

사용자 매뉴얼

상표 및 저작권

상표

Windows는 미국 및 다른 나라에서 **Microsoft Corporation**의 등록상표입니다.

다른 모든 브랜드 및 제품명은 해당 소유자의 상표 또는 등록상표입니다.

이 설명서에서는 보호되는 상표를 따로 표시하지 않습니다. 하지만 그렇다고 해서 그러한 상표를 마음대로 사용할 수 있는 것은 아닙니다.

저작권 정보

Avira Internet Security에는 타사 공급자가 제공한 코드가 사용되었습니다. 그러한 코드를 사용할 수 있게 해준 저작권 소유자에게 감사드립니다.

저작권에 대한 자세한 내용은 Avira Internet Security의 프로그램 도움말에서 "타사 라이선스"를 참조하십시오.

목차

1. 소개.....	7
1.1 아이콘 및 강조 표시.....	7
2. 제품 정보.....	9
2.1 배포 범위.....	9
2.2 시스템 요구 사항.....	10
2.3 라이선스 및 업그레이드.....	12
2.3.1 라이선스.....	12
2.3.2 라이선스 연장.....	12
2.3.3 업그레이드.....	12
2.3.4 라이선스 관리자.....	13
3. 설치 및 제거.....	15
3.1 설치 유형.....	15
3.2 설치 전 작업.....	16
3.3 빠른 설치.....	17
3.4 사용자 지정 설치.....	20
3.5 테스트 제품 설치.....	23
3.6 구성 마법사.....	25
3.7 설치 변경.....	26
3.8 설치 모듈.....	26
3.9 제거.....	28
4. Avira Internet Security 개요.....	29
4.1 사용자 인터페이스 및 작업.....	29
4.1.1 제어 센터.....	29
4.1.2 게임 모드.....	33
4.1.3 구성.....	33
4.1.4 트레이 아이콘.....	37
4.2 Avira SearchFree Toolbar.....	39
4.2.1 사용.....	39

4.2.2	옵션.....	43
4.2.3	제거.....	46
4.3	방법.....	48
4.3.1	라이선스 활성화.....	48
4.3.2	제품 정품 인증.....	49
4.3.3	자동 업데이트 수행.....	50
4.3.4	수동 업데이트 시작.....	51
4.3.5	검사 프로필을 사용한 바이러스 및 맬웨어 검사.....	52
4.3.6	끌어서 놓기를 사용한 바이러스 및 맬웨어 검사.....	54
4.3.7	상황에 맞는 메뉴를 사용한 바이러스 및 맬웨어 검사.....	54
4.3.8	바이러스 및 맬웨어 자동 검사.....	55
4.3.9	Rootkits 및 활성 맬웨어에 대한 대상 지정 검사.....	56
4.3.10	검색한 바이러스 및 맬웨어에 대응.....	57
4.3.11	격리된 파일(*.qua) 처리.....	62
4.3.12	격리 저장소의 파일 복원.....	64
4.3.13	의심스러운 파일을 격리 저장소로 이동.....	66
4.3.14	검사 프로필의 파일 형식 수정 또는 삭제.....	66
4.3.15	검사 프로필의 바탕 화면 바로 가기 만들기.....	67
4.3.16	이벤트 필터링.....	67
4.3.17	검사에서 전자 메일 주소 제외.....	68
4.3.18	스팸 방지 모듈 학습.....	69
4.3.19	FireWall의 보안 수준 선택.....	69
4.3.20	수동으로 백업 만들기.....	70
4.3.21	자동 데이터 백업 만들기.....	72
5.	Scanner.....	75
6.	업데이트.....	76
7.	FireWall.....	78
8.	Backup.....	79
9.	FAQ, 팁.....	80
9.1	문제 발생 시 도움말.....	80
9.2	바로 가기.....	85
9.2.1	대화 상자에서.....	85
9.2.2	도움말에서.....	86
9.2.3	제어 센터에서.....	87

- 9.3 Windows 보안 센터 90
 - 9.3.1 일반.....90
 - 9.3.2 Windows 보안 센터와 Avira 제품90
- 9.4 Windows 관리 센터 94
 - 9.4.1 일반.....94
 - 9.4.2 Windows 관리 센터와 Avira 제품94
- 10. 바이러스 및 기타 101**
 - 10.1 위협 범주 101
 - 10.2 바이러스 및 기타 맬웨어 105
- 11. 정보 및 서비스 109**
 - 11.1 연락처 주소 109
 - 11.2 기술 지원 109
 - 11.3 의심스러운 파일..... 110
 - 11.4 오진 보고 110
 - 11.5 보안 강화를 위한 사용자 의견 보내기 110
- 12. 참조: 구성 옵션 111**
 - 12.1 Scanner 111
 - 12.1.1 검사..... 111
 - 12.1.2 보고서 120
 - 12.2 Real-Time Protection..... 121
 - 12.2.1 검사..... 121
 - 12.2.2 보고서 132
 - 12.3 업데이트 133
 - 12.3.1 웹 서버 134
 - 12.4 Backup..... 136
 - 12.4.1 설정..... 136
 - 12.4.2 예외..... 136
 - 12.4.3 보고서 139
 - 12.5 FireWall..... 139
 - 12.5.1 FireWall 구성 139
 - 12.5.2 Avira FireWall 139
 - 12.6 Web Protection 165
 - 12.6.1 검사..... 165

12.6.2	보고서	173
12.7	Mail Protection	174
12.7.1	검사.....	174
12.7.2	일반.....	181
12.7.3	보고서	185
12.8	자녀 보호	186
12.8.1	Safe Browsing	186
12.9	모바일 보호	195
12.9.1	모바일 보호	195
12.10	일반	195
12.10.1	위험 범주.....	195
12.10.2	고급 보호 기능.....	196
12.10.3	암호.....	200
12.10.4	보안.....	202
12.10.5	WMI	204
12.10.6	이벤트	204
12.10.7	보고서	205
12.10.8	디렉터리	205
12.10.9	음향 알림.....	206
12.10.10	알림.....	207

1. 소개

Avira 제품은 컴퓨터를 바이러스, 웜, 트로이 목마, 애드웨어와 스파이웨어 및 기타 위험으로부터 보호합니다. 이 설명서에서는 이를 바이러스나 맬웨어(유해 소프트웨어) 및 사용자 동의 없이 설치된 프로그램으로 지칭합니다.

프로그램 설치 및 작동에 대해서는 설명서에서 설명합니다.

추가적인 옵션과 정보에 대해서는 웹 사이트를 참조하십시오.

<http://www.avira.kr>

Avira 웹 사이트에서 제공하는 기능:

- Avira 데스크톱 프로그램에 대한 정보 액세스
- 최신 Avira 데스크톱 프로그램 다운로드
- PDF 형식의 최신 제품 설명서 다운로드
- 무료 지원 및 복구 도구 다운로드
- 포괄적 기술 자료 데이터베이스와 문제 해결 FAQ 액세스
- 국가별 지원 주소에 액세스

Avira 팀 드림

1.1 아이콘 및 강조 표시

다음 아이콘이 사용됩니다.

아이콘/명칭	설명
✓	작업을 실행하기 전에 충족되어야 하는 조건 앞에 표시됩니다.
▶	사용자가 수행하는 작업 단계 앞에 표시됩니다.
↪	이전 작업 다음에 오는 이벤트 앞에 표시됩니다
경고	심각한 데이터 손실이 발생할 수 있을 때 경고 앞에 표시됩니다.

참고	Avira 제품을 더 쉽게 이용하는 데 도움이 되는 특히 중요한 정보나 팁의 링크 앞에 표시됩니다.
----	---

다음 강조 표시가 사용됩니다.

강조 표시	설명
기울임꼴	파일 이름 또는 경로 데이터입니다.
	표시된 소프트웨어 인터페이스 요소(예: 창 섹션 또는 오류 메시지)입니다.
굵게	클릭 가능한 소프트웨어 인터페이스 요소입니다(예: 메뉴 항목, 탐색 영역, 옵션 상자 또는 버튼).

2. 제품 정보

이 장에서는 Avira 제품의 구입과 사용에 관한 모든 정보를 제공합니다.

- 참조: [배포 범위](#)
- 참조: [시스템 요구 사항](#)
- 참조: [라이선스 및 업그레이드](#)
- 참조: [라이선스 관리자](#)

Avira 제품은 바이러스, 맬웨어, 사용자 동의 없이 설치된 프로그램 및 기타 위험으로부터 컴퓨터를 보호할 수 있는 포괄적이고 유연한 도구입니다.

▶ 다음 사항에 유의하십시오.

경고

대부분의 경우 중요한 데이터가 손실되면 막대한 결과가 초래됩니다. 가장 뛰어난 바이러스 차단 프로그램이라도 데이터 손실을 100% 막을 수는 없습니다. 따라서 보안을 유지하려면 정기적으로 데이터의 복사본(백업)을 만드십시오.

참고

프로그램이 바이러스, 맬웨어, 사용자 동의 없이 설치된 프로그램 및 기타 위험으로부터 효과적이고 안정적으로 보호하기 위해서는 최신 버전이어야 합니다. 자동 업데이트를 통해 Avira 제품을 최신 상태로 유지하십시오. 그에 따라 프로그램을 구성하십시오.

2.1 배포 범위

Avira 제품의 기능:

- 전체 프로그램을 모니터링, 관리 및 제어하는 제어 센터
- 사용하기 편리한 표준 및 고급 옵션 그리고 상황에 맞는 도움말을 이용하는 중앙 관리식 구성
- 알려진 모든 유형의 바이러스 및 맬웨어를 검사하는 **Scanner**(수동 검사), 이 검사는 프로필을 통해 제어 및 구성 가능
- **Windows Vista** 사용자 계정 제어와 통합할 경우, 관리 권한이 필요한 작업을 수행할 수 있습니다.
- 모든 파일 액세스 시도를 지속적으로 모니터링하는 **Real-Time Protection**(실시간 검사)

- 프로그램 작업을 지속적으로 모니터링하는 **ProActiv** 구성 요소(32비트 시스템에만 해당)
- 전자 메일 첨부 파일 검사를 포함하여, 전자 메일의 바이러스 및 맬웨어를 영구적으로 검사하는 **Mail Protection(POP3 Scanner, IMAP Scanner 및 SMTP Scanner)**
- 빠르고 편리한 검색 옵션을 제공하는 웹 브라우저 통합 검색 toolbar인 **Avira SearchFree Toolbar**입니다. 자주 사용하는 인터넷 기능의 위젯도 포함되어 있습니다.
- **HTTP** 프로토콜을 사용하여 인터넷에서 전송되는 데이터 및 파일을 모니터링하기 위한 **Web Protection(포트 80, 8080, 3128의 모니터링)**
- 역할을 기반으로 바람직하지 않은 웹 사이트를 필터링하고 인터넷 사용을 제한하는 자녀 보호 구성 요소
- **Avira Free Android Security** 앱은 도난 방지 대책에만 도움이 되는 것은 아닙니다. 이 앱은 모바일 장치를 잃어버렸거나 도난 당한 경우 되찾는 데 도움이 됩니다. 또한 수신 통화나 **SMS**를 차단할 수도 있습니다. **Avira Free Android Security**는 **Android** 운영 체제를 실행하는 휴대 전화와 스마트폰을 보호합니다.
- 데이터 백업을 만드는 백업 구성 요소(미러 백업)
- 통합 격리 저장소 관리로 의심스러운 파일 격리 및 처리
- 컴퓨터 시스템에서 설치된 숨겨진 맬웨어(**Rootkits**)를 탐지하기 위한 **Rootkits protection (Windows XP 64비트)**
- 검색된 바이러스 및 맬웨어에 대한 자세한 정보를 인터넷을 통해 직접 확인
- 인터넷 웹 서버 또는 을 이용하는 단일 파일 업데이트 및 증분형 **VDF** 업데이트에서 간단하고 신속하게 프로그램, 바이러스 정의 및 검색 엔진 업데이트
- 편리하게 라이선스를 관리할 수 있는 라이선스 관리자
- 일회성 또는 반복되는 작업(예: 업데이트, 검사)을 계획할 수 있는 통합형 스케줄러
- 추론 검사 방법을 비롯한 혁신적인 검사 기술(검사 엔진)을 통해 바이러스 및 맬웨어에 대해 매우 높은 검색률 달성
- 중첩된 압축 검색 및 스마트 확장명 검색을 비롯한 모든 일반 압축 유형 검색
- 여러 개의 파일을 동시에 고속 검사하는 고성능 멀티스레딩 기능
- 인터넷 또는 다른 네트워크를 통한 무단 액세스 및 허가받지 않은 사용자의 인터넷/네트워크 무단 액세스로부터 컴퓨터를 보호하는 **Avira FireWall**

2.2 시스템 요구 사항

시스템 요구 사항은 다음과 같습니다.

- 1Ghz 이상의 **Pentium** 프로세서 이상이 장착된 컴퓨터
- 운영 체제
 - Windows XP, 최신 SP(32 또는 64비트) 또는
 - Windows 7, 최신 SP(32 또는 64비트)

참고

Avira Internet Security은(는) Windows 8 인증 진행 중입니다.

- 150MB 이상의 하드 디스크 여유 공간(임시 보관에 격리 저장소를 사용할 경우 더 많은 공간 필요)
- Windows XP의 경우 512MB 이상의 RAM
- Windows 7
- 프로그램 설치 시: 관리자 권한
- 모든 설치: Windows Internet Explorer 6.0 이상
- 적절한 경우 인터넷 연결(설치 참조)

Avira SearchFree Toolbar

- 운영 체제
 - Windows XP, 최신 SP(32 또는 64비트) 또는
 - Windows 7, 최신 SP(32 또는 64비트) 또는
- 웹 브라우저
 - Windows Internet Explorer 6.0 이상
 - Mozilla Firefox 3.0 이상
 - Google Chrome 18.0 이상


참고

필요할 경우 Avira SearchFree Toolbar를 설치하기 전에 이전에 설치된 검색 toolbar를 모두 제거하십시오. 그렇지 않으면 Avira SearchFree Toolbar를 설치할 수 없습니다.

Windows Vista 사용자를 위한 정보

Windows XP에서는 많은 사용자가 관리자 권한을 가지고 작업합니다. 하지만 보안 관점에서 보면 이는 바람직하지 않습니다. 바이러스 및 사용자 동의 없이 설치된 프로그램이 컴퓨터에 쉽게 침투할 수 있기 때문입니다.

이런 이유 때문에 Microsoft에서는 Windows Vista에 "사용자 계정 컨트롤"을 도입했습니다. 이 기능은 관리자로 로그인한 사용자에게 더 많은 보호를 제공하며 따라서 Windows Vista에서 처음에는 관리자가 일반 사용자의 권한만 가집니다. 관리자 권한이 필요한 작업은 Windows Vista에서 정보 아이콘으로 명확하게 표시됩니다. 또한 이 사용자는 요청된 작업을 명시적으로 확인해야 합니다. 그래야만 권한이 상승되며 이 권한을 받아야만 운영 체제가 관리 작업을 수행할 수 있습니다.

Windows Vista에서는 일부 작업에 대해 Avira 제품에 관리자 권한이 필요합니다. 그러한 작업은 다음 기호로 표시됩니다. . 이 기호가 버튼 위에도 나타날 경우 그 작업을 수행하려면 관리자 권한이 필요합니다. 현재 사용자 계정에 관리자 권한이 없는 경우 Windows Vista의 사용자 계정 제어 대화 상자에서 관리자 암호를 입력하라는 메시지를 표시합니다. 관리자 암호를 입력하지 않을 경우 이 작업을 수행할 수 없습니다.

2.3 라이선스 및 업그레이드

2.3.1 라이선스

Avira 제품을 사용하려면 라이선스가 필요합니다. 따라서 라이선스 조건에 동의해야 합니다.

라이선스는 정품 인증 키의 형태로 제공됩니다. 정품 인증 코드는 Avira 제품 구입 후 받는 문자 및 숫자로 구성된 코드입니다. 이 정품 인증 코드에는 정확한 라이선스 데이터, 즉 사용이 허가된 프로그램 및 그 기간에 대한 정보가 포함되어 있습니다.

Avira 제품을 인터넷에서 또는 제품 패키지를 통해 구입한 경우 정품 인증 코드가 전자 메일로 전송됩니다.

프로그램 사용을 허가 받으려면 정품 인증 코드를 입력하여 프로그램을 정품 인증하십시오. 제품 인증은 설치 시 수행할 수 있습니다. 하지만 Avira 제품을 설치한 후 **도움말 > 라이선스 관리**에서 라이선스 관리자를 통해 인증할 수도 있습니다.

2.3.2 라이선스 연장

라이선스 만료가 임박한 경우 Avira에서 라이선스 연장이 필요함을 알리는 슬라이드업을 전송할 것입니다. 라이선스를 연장하려면 링크를 클릭하십시오. 그러면 Avira 온라인 쇼핑몰로 이동합니다. 다른 한편으로, **도움말 > 라이선스 관리** 아래에서 라이선스 관리자를 통해 Avira 제품의 라이선스를 연장할 수도 있습니다.

Avira의 라이선싱 포털에 등록된 경우 **라이선스 개요**를 통해 온라인으로 직접 라이선스를 추가로 연장하거나 라이선스 자동 갱신을 선택할 수 있습니다.

2.3.3 업그레이드

라이선스 관리자에서는 Avira 데스크톱 제품군에서 제품에 대한 업그레이드를 시작할 수 있습니다. 이전 제품을 수동으로 제거하고 새 제품을 수동으로 설치할 필요가 없습니다. 라이선스 관리자에서 업그레이드할 때는 라이선스 관리자 입력란에 업그레이드할 제품의 정품 인증 코드를 입력합니다. 그러면 새 제품이 자동으로 설치됩니다.

컴퓨터의 높은 안정성과 보안을 위해, **Avira**는 시스템을 최신 버전으로 업그레이드하라는 안내를 팝업으로 표시합니다. 팝업 항목에서 **업그레이드** 링크를 클릭하기만 하면 제품별 업그레이드 사이트로 연결됩니다.

현재 제품을 업그레이드하거나 더 포괄적인 제품을 구입할 수도 있습니다. 제품 개요 페이지에서 지금 사용 중인 제품의 개요를 볼 수 있으며 현재 제품을 다른 **Avira** 제품과 비교할 수 있습니다. 더 자세한 정보가 필요하면 제품 이름 오른쪽의 **정보** 아이콘을 클릭하십시오. 같은 제품을 계속 사용하려면 **업그레이드**를 클릭하십시오. 그러면 새 버전의 다운로드가 즉시 시작됩니다. 더 포괄적인 제품을 구입하려면 제품 열 하단의 **구입** 버튼을 클릭하십시오. 그러면 자동으로 구매 주문을 할 수 있는 **Avira** 온라인 쇼핑몰로 이동합니다.

참고

제품 및 운영 체제에 따라 업그레이드를 수행하려면 관리자 권한이 필요할 수 있습니다. 업그레이드를 수행하기 전에 관리자로 로그인하십시오.

2.3.4 라이선스 관리자

Avira Internet Security 라이선스 관리자를 사용하면 **Avira Internet Security** 라이선스를 간편하게 설치할 수 있습니다.

Avira Internet Security 라이선스 관리자



파일 관리자 또는 정품 인증 전자 메일에서 라이선스 파일을 더블클릭하여 선택하고 화면의 안내에 따라 라이선스를 설치할 수 있습니다.

참고

Avira Internet Security 라이선스 관리자는 자동으로 해당 라이선스를 각 제품 폴더에 복사합니다. 라이선스가 이미 있는 경우 기존 라이선스 파일 대체 여부에 관한 메시지가 나타납니다. 이 경우에는 기존 파일을 새 라이선스 파일이 덮어씁니다.

3. 설치 및 제거

이 장에서는 Avira 제품의 설치 및 제거에 대해 설명합니다.

- 참조: [사전 설치](#): 설치 요구 사항 및 준비
- 참조: [빠른 설치](#): 기본 설정에 따라 표준 설치
- 참조: [사용자 지정 설치](#): 구성 가능한 설치
- 참조: [테스트 제품 설치](#)
- 참조: [구성 마법사](#)
- 참조: [설치 변경](#)
- 참조: [설치 모듈](#)
- 참조: [제거](#): 제거

3.1 설치 유형

설치하는 동안 설치 마법사에서 설치 유형을 선택할 수 있습니다.

빠른 설치

- 표준 구성 요소가 설치됩니다.
- 프로그램 파일은 *C:\Program Files*의 기본 폴더에 설치됩니다.
- Avira 제품은 기본 설정으로 설치됩니다. 구성 마법사를 사용하여 사용자 지정 설정을 정의할 수 있습니다.

사용자 지정

- 개별 프로그램 구성 요소를 설치하도록 선택할 수 있습니다([설치 및 제거 > 설치 모듈](#) 참조).
- 프로그램 파일이 설치된 대상 폴더를 선택할 수 있습니다.
- 시작 메뉴에서 **바탕 화면 아이콘** 및 **프로그램 그룹 만들기** 옵션의 선택을 취소할 수 있습니다.
- 구성 마법사를 사용하여 Avira 제품에 대한 사용자 지정 설정을 정의하고 설치 후 자동으로 수행되는 기본 시스템 검사를 시작할 수 있습니다.

3.2 설치 전 작업

참고

설치하기 전에 컴퓨터가 모든 **최소 시스템 요구 사항**을 충족하는지 확인하십시오. 컴퓨터가 모든 요구 사항을 충족할 경우 **Avira** 제품을 설치할 수 있습니다.

설치 전 작업

- ✓ 전자 메일 프로그램을 닫습니다. 실행 중인 응용 프로그램을 모두 종료하는 것이 좋습니다.
- ✓ 다른 어떤 바이러스 백신 솔루션도 설치되지 않았어야 합니다. 여러 보안 솔루션의 자동 보호 기능이 서로 충돌할 수 있습니다.
 - ↳ **Avira** 제품에서 컴퓨터에 호환되지 않는 소프트웨어가 있는지 검색합니다.
 - ↳ 호환되지 않는 소프트웨어가 발견될 경우 이러한 프로그램 목록이 생성됩니다.
 - ↳ 컴퓨터의 안정성을 유지하기 위해 이러한 소프트웨어를 제거하는 것이 좋습니다.
- ▶ 컴퓨터에서 자동으로 제거해야 할 이러한 모든 프로그램의 체크박스를 목록에서 선택하고 **다음**을 클릭합니다.
- ▶ 일부 프로그램의 경우에는 제거를 수동으로 확인해야 합니다. 프로그램을 선택하고 **다음**을 클릭합니다.
 - ↳ 선택한 프로그램 중 하나 이상을 제거하려면 컴퓨터를 다시 시작해야 합니다. 재부팅한 후 설치가 계속됩니다.

경고

Avira 제품의 설치가 완료될 때까지는 컴퓨터가 보호되지 않습니다.

설치

설치 프로그램은 설명이 따로 필요 없는 대화 상자 모드로 실행됩니다. 모든 창에는 설치 프로세스를 제어하는 특정 버튼이 포함되어 있습니다.

대표적인 은 다음과 같습니다.

- **확인**: 작업을 확인합니다.
- **중단**: 작업을 중단합니다.
- **다음**: 다음 단계로 이동합니다.
- **뒤로**: 이전 단계로 이동합니다.

- ▶ 인터넷 연결 설정: 다음 설치 단계를 수행하려면 인터넷 연결이 필요합니다.
- 설치 프로그램을 통해 최신 프로그램 파일과 최신 바이러스 정의 파일 다운로드(인터넷 기반 설치용)
- 프로그램 정품 인증
- 해당되는 경우 설치를 마친 후 업데이트 수행
- ▶ 프로그램을 정품 인증하려는 경우 Avira 제품의 정품 인증 코드나 라이선스 파일을 가까운 곳에 보관합니다.

참고

인터넷 기반 설치:

프로그램의 인터넷 기반 설치에서는 설치에 앞서 Avira 웹 서버에서 최신 프로그램을 로드하는 인터넷 기반 설치 프로그램을 제공합니다. 이 프로세스를 수행하면 Avira 제품이 최신 바이러스 정의 파일과 함께 설치됩니다.

설치 패키지로 설치:

설치 패키지에는 설치 프로그램과 필요한 모든 프로그램 파일이 들어 있습니다. 설치 패키지로 설치하는 경우 Avira 제품에 대한 언어를 선택할 수 없습니다. 설치 후에 바이러스 정의 파일을 업데이트하는 것이 좋습니다.

참고

정품 인증 시 Avira 제품은 HTTP 프로토콜과 포트 80(웹 통신) 및 암호화 프로토콜 SSL과 포트 443을 사용하여 Avira 서버와 통신합니다. FireWall을 사용 중인 경우 필요한 연결 및/또는 보내거나 받는 데이터가 FireWall에 의해 차단되지 않도록 하십시오.

3.3 빠른 설치

Avira 제품 설치:

인터넷에서 다운로드한 설치 파일을 더블클릭하여 설치 프로그램을 시작하거나 프로그램 CD를 넣습니다.

인터넷 기반 설치

- 시작 화면이 나타납니다.
- ▶ 다음을 클릭하여 설치를 계속 진행합니다.
- 언어 선택 대화 상자가 나타납니다.

- ▶ Avira 제품을 설치하는 데 사용할 언어를 선택하고 다음을 클릭하여 언어 선택을 확인합니다.
 - ↳ 다운로드 대화 상자가 나타납니다. Avira 웹 서버에서 설치에 필요한 모든 파일이 다운로드됩니다. 다운로드가 끝나면 다운로드 창이 닫힙니다.

설치 패키지로 설치

- ↳ 설치 준비 창이 나타납니다.
- ↳ 설치 파일이 추출됩니다. 설치 루틴이 시작됩니다.
- ↳ 설치 유형 선택 대화 상자가 나타납니다.

참고

기본적으로 빠른 설치가 미리 설정되어 있습니다. 사용자가 구성할 수 없는 모든 표준 구성 요소가 설치됩니다. 사용자 지정 설치를 실행하려는 경우 [설치 및 제거 > 사용자 지정 설치](#) 장을 참조하십시오.

- ▶ **Avira Proactiv 및 Protection Cloud를 사용하여 보호를 개선하고 싶습니다.**
 체크박스([구성 > 일반 > 고급 보호](#))가 기본적으로 미리 설정되어 있습니다. Avira 커뮤니티에 참여하기를 원치 않으면 이 체크박스의 선택을 취소하십시오.
 - ↳ Avira 커뮤니티에 참여하기로 한 경우 Avira에서 검색된 의심스러운 프로그램에 대한 데이터를 Avira 맬웨어 연구 센터로 보냅니다. 이 데이터는 고급 온라인 검사와 검색 기술을 확장하고 조정하는 용도로만 사용됩니다. **ProActiv** 및 **Protection Cloud** 링크를 클릭하면 고급 온라인 및 클라우드 검사에 대한 자세한 내용을 볼 수 있습니다.
- ▶ **최종 사용자 사용권 계약에 동의합니다. 최종 사용자 사용권 계약의 자세한 내용을 읽어보려면 EULA 링크를 클릭합니다.**
 - ↳ 라이선스 마법사가 표시되어 제품 인증을 도와줍니다.
 - ↳ 여기서는 곧바로 프록시 서버를 구성할 수 있습니다.
- ▶ 필요할 경우 구성할 **프록시 설정**을 클릭하고 **확인**을 눌러 설정을 확인합니다.
- ▶ 이미 인증 코드를 받은 경우 **제품 인증**을 선택하고 인증 코드를 입력합니다.
 -또는-
- ▶ 정품 인증 코드가 없는 경우 **정품 인증 코드 구매** 링크를 클릭합니다.
 - ↳ Avira 웹 사이트에 연결됩니다.
 - 또는 **유효한 라이선스 파일 있음** 링크를 클릭합니다.
 - ↳ **파일 열기** 대화 상자가 나타납니다.
- ▶ **.KEY** 라이선스 파일을 선택하고 **열기**를 클릭합니다.

- 정품 인증 코드가 라이선스 마법사로 복사됩니다.
- ▶ 제품을 테스트하려는 경우 계속해서 **제품 평가 설치** 장을 읽어 보십시오.
- ▶ 다음을 클릭합니다.
 - 설치 진행률이 녹색 막대로 표시됩니다.
- ▶ 다음을 클릭합니다.
 - **Avira SearchFree**를 이미 사용하는 수백만명 **Avira** 사용자가 가입한 커뮤니티에 참여 대화 상자가 나타납니다.
- ▶ Avira SearchFree Toolbar를 설치하기를 원치 않는 경우 Avira SearchFree Toolbar 및 Avira SearchFree Updater **최종 사용자 사용권 계약** 체크박스과 **Avira SearchFree(search.avira.com)**를 브라우저 홈 페이지로 정의하는 체크박스의 선택을 취소하십시오.

참고
 필요할 경우 Avira SearchFree Toolbar를 설치하기 전에 이전에 설치된 검색 toolbar를 모두 제거하십시오. 그렇지 않으면 Avira SearchFree Toolbar를 설치할 수 없습니다.

- ▶ 다음을 클릭합니다.
 - Avira SearchFree Toolbar의 설치 진행률이 녹색 막대로 표시됩니다.
 - Avira 트레이 아이콘은 작업 표시줄에 있습니다.
 - 컴퓨터에 대한 유효한 보호 상태를 유지하기 위해 **업데이트 프로그램** 모듈에서 사용 가능한 업데이트가 있는지 검색합니다.
 - **Luke Filewalker** 창이 열리고 간단한 시스템 검사가 수행됩니다. 검사 상태와 결과가 표시됩니다.
- ▶ 검사 후에 컴퓨터를 다시 시작할지 묻는 메시지가 표시되면 **예**를 클릭하여 시스템이 완전히 보호되도록 합니다.

정상적으로 설치한 후에는 제어 센터의 **상태** 항목에서 프로그램이 최신 상태인지 확인하는 것이 좋습니다.

- ▶ Avira 제품에 컴퓨터가 안전하지 않다는 메시지가 표시되면 **문제 수정**을 클릭하십시오.
 - 그러면 **보호 복원** 대화 상자가 열립니다.
- ▶ 시스템의 보안을 최대화하기 위해 사전 설정 옵션을 활성화합니다.
- ▶ 적절한 경우 전체 시스템 검사를 수행합니다.

3.4 사용자 지정 설치

Avira 제품 설치:

인터넷에서 다운로드한 설치 파일을 더블클릭하여 설치 프로그램을 시작하거나 프로그램 CD를 넣습니다.

인터넷 기반 설치

- 시작 화면이 나타납니다.
- ▶ 다음을 클릭하여 설치를 계속 진행합니다.
 - 언어 선택 대화 상자가 나타납니다.
- ▶ Avira 제품을 설치하는 데 사용할 언어를 선택하고 다음을 클릭하여 언어 선택을 확인합니다.
 - 다운로드 대화 상자가 나타납니다. Avira 웹 서버에서 설치에 필요한 모든 파일이 다운로드됩니다. 다운로드가 끝나면 다운로드 창이 닫힙니다.

설치 패키지로 설치

- 설치 준비 창이 나타납니다.
- 설치 파일이 추출됩니다. 설치 루틴이 시작됩니다.
- 설치 유형 선택 대화 상자가 나타납니다.

참고

기본적으로 빠른 설치가 미리 설정되어 있습니다. 사용자가 구성할 수 없는 모든 표준 구성 요소가 설치됩니다. 빠른 설치를 실행하려는 경우 [설치 및 제거 > 빠른 설치](#) 장을 참조하십시오.

- ▶ 개별 프로그램 구성 요소를 설치하려면 사용자 지정을 선택합니다.
- ▶ **Avira Proactiv 및 Protection Cloud**를 사용하여 보호를 개선하고 싶습니다. 체크박스가 기본적으로 미리 설정되어 있습니다. Avira 커뮤니티에 참여하고 싶지 않으면 이 체크박스의 선택을 취소하십시오.
 - Avira 커뮤니티에 참여하기로 한 경우 Avira에서 검색된 의심스러운 프로그램에 대한 데이터를 Avira 맬웨어 연구 센터로 보냅니다. 이 데이터는 고급 온라인 검사와 검색 기술을 확장하고 조정하는 용도로만 사용됩니다. **ProActiv 및 Protection Cloud** 링크를 클릭하면 고급 온라인 및 클라우드 검사에 대한 자세한 내용을 볼 수 있습니다.
- ▶ 최종 사용자 사용권 계약에 동의합니다. 최종 사용자 사용권 계약의 자세한 내용을 읽어보려면 EULA 링크를 클릭합니다.

- ▶ 다음을 클릭합니다.
 - ↳ 대상 폴더 선택 창이 열립니다.
 - ↳ 기본 폴더는 `C:\Program Files\Avira\AntiVir Desktop`입니다.
- ▶ 계속하려면 다음을 클릭합니다.
 - 또는-
 - 찾아보기 버튼을 사용하여 다른 대상 폴더를 선택하고 다음을 클릭하여 확인합니다.
 - ↳ 구성 요소 설치 대화 상자가 나타납니다.
- ▶ 목록에서 구성 요소를 선택하거나 선택을 취소하고 다음을 클릭하여 계속 진행합니다.
- ▶ **Protection Cloud** 구성 요소를 설치하도록 선택했지만 클라우드로 전송하여 분석할 파일을 수동으로 확인하려면 **의심스러운 파일을 Avira에 보낼 때 수동으로 확인** 옵션을 사용하도록 설정할 수 있습니다.
- ▶ 다음을 클릭합니다.
- ▶ 다음 대화 상자에서는 바탕 화면 바로 가기 및/또는 시작 메뉴의 프로그램 그룹을 만들 것인지 선택할 수 있습니다.
- ▶ 다음을 클릭합니다.
 - ↳ 라이선스 마법사가 표시됩니다.

프로그램을 정품 인증할 때 다음 옵션 중에서 선택할 수 있습니다.

- ▶ 정품 인증 코드를 입력합니다.
 - ↳ 정품 인증 코드를 입력하면 Avira 제품이 해당 라이선스로 정품 인증됩니다.
- ▶ 정품 인증 코드가 없는 경우 정품 인증 코드 구매 링크를 클릭합니다.
 - ↳ Avira 웹 사이트에 연결됩니다.
- ▶ 제품 평가 옵션을 선택합니다.
 - ↳ 제품 평가를 선택할 경우 정품 인증 프로세스 중에 프로그램을 정품 인증하기 위한 평가판 라이선스가 생성됩니다. 특정 기간 동안 Avira 제품의 모든 기능을 테스트할 수 있습니다([제품 평가 설치 참조](#)).

참고

유효한 라이선스 파일 있음 옵션을 사용하여 유효한 라이선스 파일을 로드할 수 있습니다. 유효한 정품 인증 코드를 사용하여 정품 인증을 받는 동안 라이선스 키가 생성되어 Avira 제품의 프로그램 디렉터리에 저장되고 로드됩니다. 이미 정품 인증을 한 제품을 다시 설치할 경우 이 옵션을 사용하지 마세요.

참고

Avira 제품의 일부 판매용 버전의 경우 정품 인증 코드가 제품에 이미 포함되어 있습니다. 그러한 경우 정품 인증 절차가 필요하지 않습니다. 필요한 경우 라이선스 마법사에 정품 인증 코드가 표시됩니다.

참고

프로그램을 정품 인증하기 위해 Avira 서버와의 연결이 설정됩니다. **프록시 설정**에서 프록시 서버에 의한 인터넷 링크를 구성할 수 있습니다.

- ▶ 정품 인증 프로세스를 선택하고 **다음**을 클릭하여 확인합니다.
- ▶ 이미 유효한 라이선스 파일이 있는 경우에는 곧바로 "**유효한 라이선스 파일 있음 옵션 선택**" 장으로 이동하십시오.

제품 정품 인증

- ↳ 개인 데이터를 입력할 수 있는 대화 상자가 표시됩니다.
- ▶ 데이터를 입력하고 **다음**을 클릭합니다.
 - ↳ 데이터가 Avira 서버로 전송되고 검사됩니다. Avira 제품이 해당 라이선스로 정품 인증됩니다.
 - ↳ 라이선스 데이터가 다음 창에 표시됩니다.
- ▶ **다음**을 클릭합니다.
- ▶ "**유효한 라이선스 파일 있음 옵션 선택**"에 대한 다음 장으로 이동합니다.

"유효한 라이선스 파일 있음" 옵션 선택

- ↳ 라이선스 파일을 로드하기 위한 상자가 표시됩니다.
- ▶ 프로그램의 라이선스 데이터를 사용하여 **.KEY** 라이선스 파일을 선택하고 **열기**를 클릭합니다.
 - ↳ 라이선스 데이터가 다음 창에 표시됩니다.
- ▶ **다음**을 클릭합니다.

정품 인증 완료 또는 라이선스 파일 로드 후 계속

- ↳ **Avira SearchFree**를 이미 사용하는 수백만명 Avira 사용자가 가입한 커뮤니티에 참여 대화 상자가 나타납니다.
- ▶ Avira SearchFree Toolbar를 설치하기를 원치 않는 경우 Avira SearchFree Toolbar 및 Avira SearchFree Updater **최종 사용자 사용권 계약** 체크박스과 **Avira**

SearchFree(search.avira.com)를 브라우저 홈 페이지로 정의하는 체크박스의 선택을 취소하십시오.

참고 필요할 경우 **Avira SearchFree Toolbar**를 설치하기 전에 이전에 설치된 검색 toolbar를 모두 제거하십시오. 그렇지 않으면 **Avira SearchFree Toolbar**를 설치할 수 없습니다.

- ▶ 다음을 클릭합니다.
 - 설치 마법사가 닫히고 **구성 마법사**가 표시됩니다.

3.5 테스트 제품 설치

Avira 제품 설치:

인터넷에서 다운로드한 설치 파일을 더블클릭하여 설치 프로그램을 시작하거나 프로그램 CD를 넣습니다.

인터넷 기반 설치

- 시작 화면이 나타납니다.
- ▶ 다음을 클릭하여 설치를 계속 진행합니다.
 - 언어 선택 대화 상자가 나타납니다.
- ▶ Avira 제품을 설치하는 데 사용할 언어를 선택하고 다음을 클릭하여 언어 선택을 확인합니다.
 - 다운로드 대화 상자가 나타납니다. Avira 웹 서버에서 설치에 필요한 모든 파일이 다운로드됩니다. 다운로드가 끝나면 **다운로드** 창이 닫힙니다.

설치 패키지로 설치

- 설치 준비 창이 나타납니다.
- 설치 파일이 추출됩니다. 설치 루틴이 시작됩니다.
- 설치 유형 선택 대화 상자가 나타납니다.

참고

기본적으로 빠른 설치가 미리 설정되어 있습니다. 사용자가 구성할 수 없는 모든 표준 구성 요소가 설치됩니다. 사용자 지정 설치를 실행하려는 경우 [설치 및 제거 > 사용자 지정 설치](#) 장을 참조하십시오.

- ▶ **Avira Proactiv 및 Protection Cloud를 사용하여 보호를 개선하고 싶습니다.**
 체크박스(구성 > 일반 > 고급 보호)가 기본적으로 미리 설정되어 있습니다. Avira 커뮤니티에 참여하고 싶지 않으면 이 체크박스의 선택을 취소하십시오.
 - ↳ Avira 커뮤니티에 참여하기로 한 경우 Avira에서 검색된 의심스러운 프로그램에 대한 데이터를 Avira 맬웨어 연구 센터로 보냅니다. 이 데이터는 고급 온라인 검사와 검색 기술을 확장하고 조정하는 용도로만 사용됩니다. **ProActiv 및 Protection Cloud** 링크를 클릭하면 고급 온라인 및 클라우드 검사에 대한 자세한 내용을 볼 수 있습니다.
- ▶ **최종 사용자 사용권 계약에 동의합니다. 최종 사용자 사용권 계약의 자세한 내용을 읽어보려면 EULA 링크를 클릭합니다.**
- ▶ 다음을 클릭합니다.
 - ↳ 라이선스 마법사가 표시되어 제품 인증을 도와줍니다.
 - ↳ 여기서는 곧바로 **프록시 서버**를 구성할 수 있습니다.
- ▶ 구성할 **프록시 설정**을 클릭하고 **확인**을 눌러 설정을 확인합니다.
- ▶ 라이선스 마법사의 **제품 테스트** 옵션을 선택하고 다음을 클릭합니다.
- ▶ **등록 필수 항목에 데이터를 삽입합니다. Avira 뉴스레터**를 구독할지 여부를 결정하고 다음을 클릭합니다.
 - ↳ 설치 진행률이 녹색 막대로 표시됩니다.
 - ↳ **Avira SearchFree Toolbar**를 이미 사용하는 수백만 명 **Avira** 사용자가 가입한 커뮤니티에 참여 대화 상자가 나타납니다.
- ▶ Avira SearchFree Toolbar를 설치하기를 원치 않는 경우 Avira SearchFree Toolbar 및 Avira SearchFree Updater **최종 사용자 사용권 계약** 체크박스와 **Avira SearchFree(search.avira.com)**를 브라우저 홈 페이지로 정의하는 체크박스의 선택을 취소하십시오.

참고

필요할 경우 Avira SearchFree Toolbar를 설치하기 전에 이전에 설치된 검색 toolbar를 모두 제거하십시오. 그렇지 않으면 Avira SearchFree Toolbar를 설치할 수 없습니다.

- ▶ 다음을 클릭합니다.
- ▶ Avira 제품을 정품 인증하기 위해 시스템을 다시 시작하라는 메시지가 표시됩니다. 컴퓨터를 즉시 재부팅하려면 **예**를 클릭합니다.
 - ↳ Avira 트레이 아이콘은 작업 표시줄에 있습니다.
 - ↳ 평가판 라이선스 유효 기간은 **31일**입니다.

3.6 구성 마법사

사용자 정의 설치가 끝나면 구성 마법사가 열립니다. 구성 마법사에서는 Avira 제품의 사용자 지정 설정을 정의할 수 있습니다.

- ▶ 구성 마법사의 시작 창에서 **다음**을 클릭하여 프로그램의 구성을 시작합니다.
 - ↳ **AHeAD** 구성 대화 상자에서는 AHeAD 기술의 탐지 수준을 선택할 수 있습니다. 선택한 탐지 수준은 **Scanner**(수동 검사) 및 **Real-Time Protection**(실시간 검사) AHeAD 기술 설정에 사용됩니다.
- ▶ 탐지 수준을 선택하고 **다음**을 클릭하여 설치를 계속합니다.
 - ↳ 다음 **확장된 위협 범주 선택** 대화 상자에서는 지정된 위협 범주에 맞게 Avira 제품의 보호 기능을 변경할 수 있습니다.
- ▶ 추가 위협 범주를 활성화하고 **다음**을 클릭하여 설치를 계속합니다.
 - ↳ Avira FireWall 설치 모듈을 선택한 경우에는 **네트워크 액세스 및 네트워크 리소스 사용에 대한 기본 규칙** 대화 상자가 나타납니다. Avira FireWall에서 활성화된 리소스에 대한 외부 액세스 및 신뢰할 수 있는 기업의 응용 프로그램에 의한 네트워크 액세스를 허용할 것인지 정의할 수 있습니다.
- ▶ 필요한 옵션을 사용하도록 설정하고 **다음**을 클릭하여 구성을 계속합니다.
 - ↳ Avira Real-Time Protection 설치 모듈을 선택한 경우에는 **Real-Time Protection 시작 모드** 대화 상자가 나타납니다. Real-Time Protection 시작 시간을 지정할 수 있습니다. 컴퓨터가 재부팅될 때마다 Real-Time Protection이 지정된 시작 모드에서 시작됩니다.

참고

지정된 Real-Time Protection 시작 모드는 레지스트리에 저장되며 구성을 통해 변경할 수 없습니다.

참고

Real-Time Protection의 기본 시작 모드(일반 시작)를 선택하고 시작 시 로그인 프로세스가 빠르게 수행되면, 시작 시 자동으로 시작되도록 구성된 프로그램은 Real-Time Protection이 완전히 시작되기 전에 실행될 수 있으므로 이러한 프로그램은 검사되지 않을 수 있습니다.

- ▶ 필요한 옵션을 사용하도록 설정하고 **다음**을 클릭하여 구성을 계속합니다.
 - ↳ Avira Web Protection 설치 모듈을 선택한 경우 **Safe Browsing 사용** 대화 상자가 나타납니다. 컴퓨터 사용자에게 인터넷 사용에 대한 여러 가지 역할(어린이, 청소년, 성인)을 할당할 수 있습니다. **Safe Browsing**을 중지할 수도 있습니다.
- ▶ 필요한 **Safe Browsing** 설정을 정의하고 **다음**을 클릭하여 구성을 계속합니다.

- ↳ 다음 **암호 할당** 대화 상자에서는 암호를 설정하여 무단 액세스로부터 구성을 보호할 수 있습니다. 이 기능은 자녀 보호를 사용하는 경우에 특히 유용합니다.
- ↳ 다음 **시스템 검사** 대화 상자에서는 빠른 시스템 검사를 사용 또는 사용 안 함으로 설정할 수 있습니다. 빠른 시스템 검사는 구성이 완료된 후 그리고 컴퓨터가 다시 부팅되기 전에 실행되며, 실행 중인 프로그램 및 가장 중요한 시스템 파일을 대상으로 바이러스 및 맬웨어를 검사합니다.
- ▶ **빠른 시스템 검사** 옵션을 사용하거나 사용 안 함으로 설정하고 다음을 클릭하여 구성을 계속합니다.
 - ↳ 다음 대화 상자에서는 **마침**을 클릭하여 구성을 완료할 수 있습니다.
 - ↳ 지정하고 선택한 설정이 적용됩니다.
 - ↳ **빠른 시스템 검사** 옵션을 사용하도록 설정한 경우 **Luke Filewalker** 창이 표시됩니다. **Scanner**가 빠른 시스템 검사를 수행합니다.
- ▶ 검사 후 컴퓨터를 다시 시작하라는 메시지가 나타나면 시스템의 완전한 보호를 위해 **예**를 클릭하십시오.

설치에 성공했다면 **제어 센터**의 **상태** 항목에서 프로그램이 최신 상태인지 확인하는 것이 좋습니다.

- ▶ Avira 제품에 컴퓨터가 안전하지 않다는 메시지가 표시되면 **문제 수정**을 클릭하십시오.
 - ↳ 그러면 **보호 복원** 대화 상자가 열립니다.
- ▶ 시스템의 보안을 최대화하기 위해 사전 설정 옵션을 활성화합니다.
- ▶ 적절한 경우 전체 시스템 검사를 수행합니다.

3.7 설치 변경

현재 설치된 Avira 제품의 개별 프로그램 구성 요소를 추가하거나 제거할 수 있습니다([설치 및 제거 > 설치 모듈](#) 참조).

현재 설치의 모듈을 추가하거나 제거하려는 경우 **Windows** 제어판의 **프로그램 추가/제거** 옵션을 사용하여 프로그램을 **변경/제거**할 수 있습니다.

Avira 제품을 선택하고 **변경**을 클릭합니다. 프로그램의 **시작** 대화 상자에서 **수정** 옵션을 선택합니다. 설치 변경 과정이 안내됩니다.

3.8 설치 모듈

사용자 지정 설치 또는 변경 설치에서는 다음 설치 모듈을 선택, 추가하거나 제거할 수 있습니다.

- **Avira Internet Security**

이 모듈에는 Avira 제품의 성공적 설치에 필요한 모든 구성 요소가 포함되어 있습니다.

- **Real-Time Protection**

Avira Real-Time Protection은 백그라운드에서 실행됩니다. 이 프로그램은 실시간 모드에서 열기, 쓰기 및 복사와 같은 작업을 수행하는 동안 파일을 모니터링하고 복구합니다. 사용자가 파일 작업(예: 문서 로드, 실행, 복사)을 수행할 Avira 제품이 자동으로 파일을 검사합니다. 파일 이름 바꾸기의 경우에는 Avira Real-Time Protection의 검사가 수행되지 않습니다.

- **Mail Protection**

Mail Protection은 사용자의 컴퓨터와 전자 메일 프로그램(메일 클라이언트)이 전자 메일을 다운로드하는 전자 메일 서버 사이의 인터페이스입니다. Mail Protection은 전자 메일 프로그램과 전자 메일 서버 간의 프록시 역할로 연결됩니다. 받는 전자 메일은 모두 이 프록시를 통해 라우팅되고 바이러스 및 사용자 동의 없이 설치된 프로그램 검사를 받은 다음 전자 메일 프로그램으로 전달됩니다. 구성에 따라 이 프로그램은 해당 전자 메일을 자동으로 처리하거나 사용자에게 어떤 작업을 수행할 것인지 묻습니다. 또한 Mail Protection은 스팸 전자 메일로부터 사용자를 안정적으로 보호할 수 있습니다.

- **Avira FireWall**

Avira FireWall은 컴퓨터의 송수신 통신을 제어합니다. 이 제품은 보안 정책에 따라 통신을 허용하거나 거부합니다.

- **Rootkits Protection**

Avira Rootkits Protection은 컴퓨터 시스템에 침투한 후에는 기존의 맬웨어 차단 방법으로는 더 이상 탐지할 수 없는 소프트웨어가 컴퓨터에 이미 설치되었는지 여부를 확인합니다.

- **ProActiv**

ProActiv 구성 요소는 응용 프로그램 작업을 모니터링하여 의심스러운 응용 프로그램 동작을 사용자에게 알립니다. 이러한 동작 기반 인식을 통해 알 수 없는 맬웨어로부터 보호할 수 있습니다. ProActiv 구성 요소는 Avira Real-Time Protection에 통합됩니다.

- **Protection Cloud**

Protection Cloud 구성 요소는 알려지지 않은 맬웨어의 동적 온라인 탐지를 위한 모듈입니다.

- **Backup**

Backup 구성 요소를 사용하면 데이터의 미리 백업을 수동 및 자동으로 만들 수 있습니다.

- **Web Protection**

인터넷을 서핑할 때는 웹 브라우저를 사용하여 웹 서버에 데이터를 요청합니다. 웹 서버에서 전송되는 데이터(HTML 파일, 스크립트 및 이미지 파일, Flash 파일, 비디오 및 음악 스트림 등)는 일반적으로 브라우저 캐시로 직접 이동되어 웹 브라우저에 표시됩니다. 즉, Avira Real-Time Protection이 수행하는 것과 같은 액세스 검사가 불가능합니다. 이로 인해 바이러스 및 사용자 동의 없이 설치된 프로그램이 사용자의 컴퓨터 시스템에 액세스할 수 있습니다. Web Protection은 데이터 전송에 사용되는 포트(80, 8080, 3128)를 모니터링하고 전송된 데이터에서 바이러스 및 사용자 동의 없이

설치된 프로그램을 검사하는 HTTP 프록시입니다. 구성에 따라 이 프로그램은 해당 파일을 자동으로 처리하거나 사용자에게 어떤 작업을 수행할 것인지 묻습니다.

- **셀 확장**

셀 확장은 Windows 탐색기의 상황에 맞는 메뉴(마우스 오른쪽 버튼)에 **Avira**를 사용하여 **선택한 파일 검사** 항목을 생성합니다. 이 항목을 통해 파일이나 디렉터리를 직접 검사할 수 있습니다.

3.9 제거

컴퓨터에서 Avira 제품을 제거하려면, Windows 제어판에서 **프로그램 추가/제거** 옵션을 사용하여 프로그램을 **변경/제거**할 수 있습니다.

Avira 제품을 제거하려면(예를 들어 Windows 7에서):

- ▶ Windows 시작 메뉴에서 **제어판**을 엽니다.
- ▶ **프로그램 및 기능**을 더블클릭합니다.
- ▶ 목록에서 Avira 제품을 선택한 다음 **제거**를 클릭합니다.
 - ↳ 프로그램을 제거할 것인지 확인하는 메시지가 표시됩니다.
- ▶ **예**를 클릭하여 확인합니다.
 - ↳ Windows 방화벽을 다시 사용하도록 설정할 것인지 묻는 메시지가 나타납니다(Avira FireWall은 비활성화됨).
- ▶ **예**를 클릭하여 확인합니다.
 - ↳ 프로그램의 모든 구성 요소가 제거됩니다.
- ▶ **마침**을 클릭하여 제거를 완료합니다.
 - ↳ 컴퓨터를 다시 시작하라는 대화 상자가 나타납니다.
- ▶ **예**를 클릭하여 확인합니다.
 - ↳ 이제 컴퓨터가 다시 시작되면 Avira 제품이 제거되고 프로그램의 모든 디렉터리, 파일 및 레지스트리 항목이 삭제됩니다.

참고

Avira SearchFree Toolbar는 제거 프로그램에 포함되지 않으며 아래 단계에 따라 따로 제거해야 합니다. Firefox에서 제거하려면 부가 기능 관리자를 통해 Avira SearchFree Toolbar를 활성화해야 합니다. 제거한 후에는 검색 toolbar가 더 이상 웹 브라우저에 통합되지 않습니다.

4. Avira Internet Security 개요

이 장에서는 Avira 제품의 기능과 작업을 개괄적으로 설명합니다.

- 참조:[사용자 인터페이스 및 작업](#)
- 참조:[Avira SearchFree Toolbar](#)
- 참조:[방법](#)

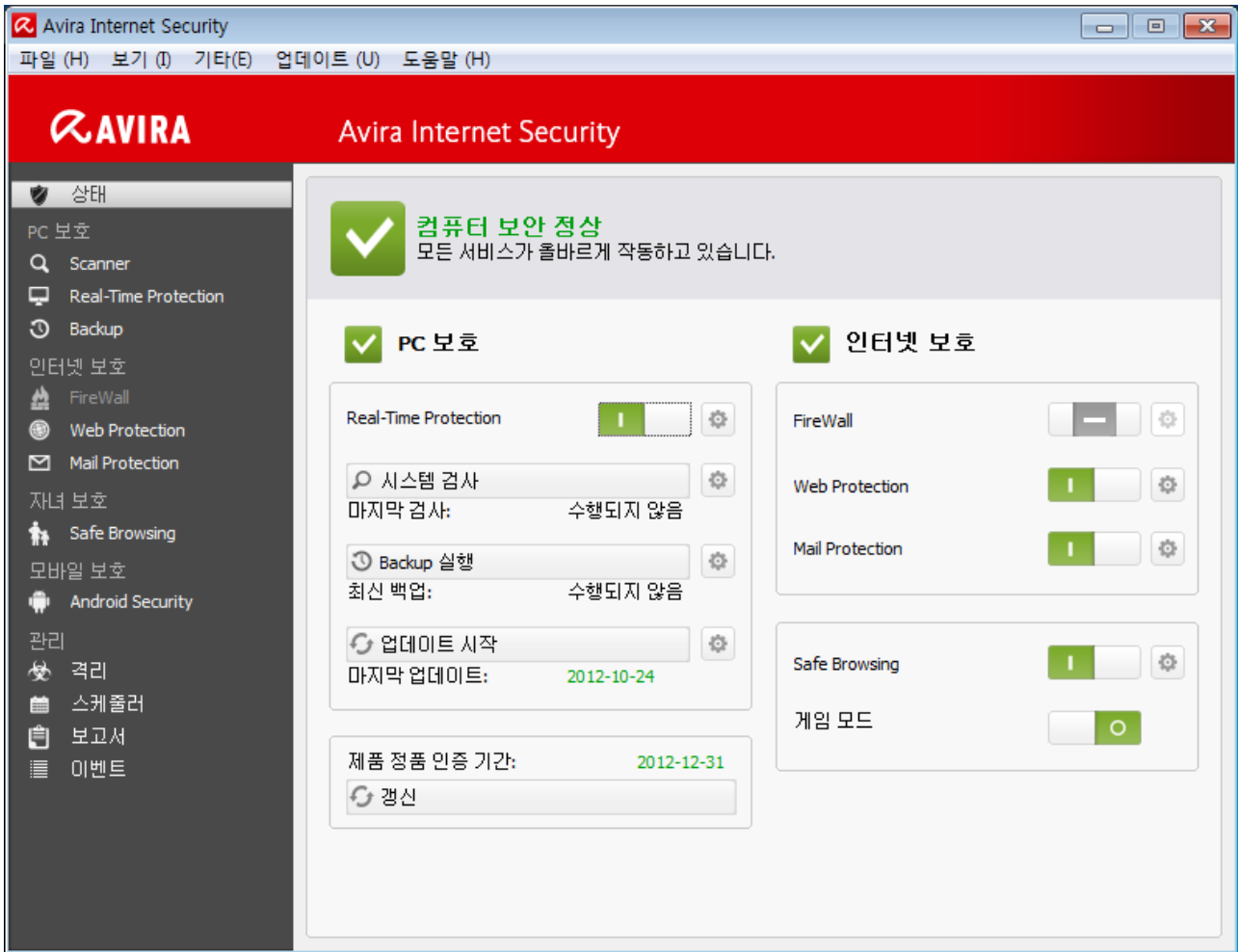
4.1 사용자 인터페이스 및 작업

Avira 제품 프로그램은 세 가지 프로그램 인터페이스 요소를 통해 사용할 수 있습니다.

- [제어 센터](#): Avira 제품의 모니터링 및 제어
- [구성](#): Avira 제품의 구성
- 작업 표시줄의 시스템 트레이에 있는 [트레이 아이콘](#): 제어 센터 및 다른 기능을 엽니다.

4.1.1 제어 센터

제어 센터는 컴퓨터 시스템의 보호 상태를 모니터링하고 Avira 제품의 보호 구성 요소 및 기능을 제어 및 작동하기 위한 용도로 설계되었습니다.



제어 센터 창은 **메뉴 모음**, **탐색 영역** 및 **상세 창 상태**의 세 영역으로 나뉩니다.

- **메뉴 모음:** 제어 센터 메뉴 모음에서는 일반 프로그램 기능 및 프로그램 정보에 액세스할 수 있습니다.
- **탐색 영역:** 탐색 영역에서서는 제어 센터의 개별 섹션 간에 손쉽게 전환할 수 있습니다. 개별 섹션에는 프로그램 구성 요소에 대한 정보와 기능이 포함되어 있으며 작업별로 탐색 모음에 정렬됩니다. 예: 작업 **PC 보호** - 섹션 **Real-Time Protection**.
- **상태:** 제어 창은 **상태** 보기에서 열리는데, 여기에서는 컴퓨터가 안전한지 여부, 활성 모듈의 개요, 마지막 백업 날짜 및 마지막 시스템 검사 날짜를 한 눈에 볼 수 있습니다. 또한 **상태** 창에는 **Real-Time Protection**의 시작이나 중지와 같은 시작 기능 또는 작업을 위한 버튼도 있습니다.

제어 센터 시작 및 종료

제어 센터를 시작하는 데 다음 옵션을 사용할 수 있습니다.

- 바탕 화면의 프로그램 아이콘 더블클릭
- 시작 > 프로그램 메뉴의 프로그램 항목을 통해
- Avira 제품의 트레이 아이콘을 통해

파일 메뉴의 닫기 메뉴 명령을 사용하거나 제어 센터의 닫기 탭을 클릭하여 제어 센터를 닫습니다.

제어 센터 작업

제어 센터를 탐색하려면

- ▶ 탐색 모음에서 작업을 선택합니다.
 - 작업이 열리고 다른 섹션이 표시됩니다. 작업의 첫 번째 섹션이 선택되고 보기에 표시됩니다.
- ▶ 필요한 경우 다른 섹션을 클릭하여 세부 정보 보기 창에 표시합니다.

참고

[Alt] 키를 사용하여 메뉴 모음에서 키보드 탐색을 활성화할 수 있습니다. 탐색이 활성화되면 **화살표** 키를 사용하여 메뉴 내에서 이동할 수 있습니다. 활성 메뉴 항목을 실행하려면 **Return** 키를 누릅니다.

제어 센터에서 메뉴를 열거나 닫을 때 또는 메뉴 내에서 탐색할 때는 "**[Alt] + 메뉴 또는 메뉴 명령에서 밑줄로 표시된 문자**" 키 조합을 사용할 수도 있습니다. 메뉴, 메뉴 명령 또는 하위 메뉴에 액세스하려면 **[Alt]** 키를 길게 누릅니다.

세부 정보 창에 표시된 데이터 또는 개체를 처리하려면 다음을 수행하십시오.

- ▶ 편집할 데이터나 개체를 강조 표시합니다.
 - 여러 요소(열의 요소)를 강조 표시하려면 **Ctrl** 키 또는 **Shift** 키를 누른 채 요소를 선택합니다.
- ▶ 세부 정보 창의 위쪽 막대에 있는 해당 버튼을 클릭하여 개체를 편집합니다.

제어 센터 개요

- **상태:** 상태 표시줄을 클릭하면 제품의 기능과 성능에 대한 개요를 볼 수 있습니다(상태 참조).
 - 상태 섹션에서는 활성 상태인 모듈을 한 눈에 볼 수 있고 마지막으로 수행된 업데이트에 대한 정보를 볼 수 있습니다.
- **PC 보호:** 이 섹션에는 컴퓨터 시스템의 파일에서 바이러스 및 맬웨어를 검사하는 구성 요소가 있습니다.
 - **Scanner** 섹션에서는 수동 검사를 손쉽게 구성하고 시작할 수 있습니다. 미리 정의된 프로필을 사용하면 미리 정의한 기본 옵션으로 검사할 수 있습니다. 같은 방법으로 수동 선택(저장되지 않음)을 사용하거나 사용자 정의 프로필을 만들어 바이러스 및 사용자 동의 없이 설치된 프로그램에 대한 검사를 개인 요구 사항에 맞게 조정할 수 있습니다.

- **Real-Time Protection** 섹션에는 검사한 파일에 대한 정보와 기타 통계 데이터가 표시되며 이러한 데이터는 언제든지 재설정할 수 있고 이를 통해 보고서 파일에 액세스할 수 있습니다. 발견된 최신 바이러스 또는 사용자 동의 없이 설치된 프로그램에 대한 세부 정보를 보려면 버튼을 누릅니다.
- **Backup** 섹션에서는 손쉽게도 신속하게 데이터 백업을 만들고 백업 작업을 시작할 수 있습니다.
- **인터넷 보호:** 이 섹션에는 인터넷의 바이러스 및 맬웨어와 권한이 없는 네트워크 액세스로부터 컴퓨터 시스템을 보호하기 위한 구성 요소가 있습니다.
 - **FireWall** 섹션에서는 **Avira FireWall**에 대한 기본 설정을 구성할 수 있습니다. 또한, 네트워크 연결을 사용하는 현재 데이터 전송 속도 및 모든 활성 응용 프로그램이 표시됩니다.
 - **Web Protection** 섹션에는 검사한 **URL** 및 탐지된 바이러스에 대한 정보와 통계 데이터가 표시되며 이 데이터는 언제나 재설정할 수 있고 이를 통해 보고서 파일에 액세스할 수 있습니다. 발견된 최신 바이러스 또는 사용자 동의 없이 설치된 프로그램에 대한 세부 정보를 보려면 버튼을 누릅니다.
 - **Mail Protection** 섹션에는 **Mail Protection**에서 검사한 모든 전자 메일, 해당 속성 및 기타 통계 데이터가 표시됩니다. 스팸 방지 필터를 조정하고 이후 맬웨어나 스팸 검사에서 전자 메일 주소를 제외할 수도 있습니다. **Mail Protection** 버퍼에서 전자 메일을 삭제할 수도 있습니다.
- **자녀 보호:** 이 섹션에는 어린이에게 안전한 인터넷 환경을 제공하기 위한 구성 요소가 들어 있습니다.
 - **Safe Browsing** 섹션에서는 컴퓨터의 사용자에게 사용자 역할을 할당할 수 있습니다. 사용자 역할은 구성 가능하며 허용 및 차단되는 **URL**, 금지되는 **URL** 범주, 인터넷 사용 시간 및 필요한 경우 허용되는 평일 사용 시간이 포함됩니다.
- **모바일 보호:** 이 섹션에서는 **Android** 장치에 대한 온라인 액세스를 리디렉션됩니다.
 - **Avira Free Android Security**는 모든 **Android** 기반 장치를 관리합니다.
- **관리:** 이 섹션에서는 의심스럽거나 감염된 파일을 격리 및 관리하고 반복되는 작업을 계획하는 도구가 제공됩니다.
 - 격리 저장소 섹션에는 격리 관리자가 포함되어 있습니다. 이 섹션은 격리 저장소에 배치된 파일 또는 격리 저장소에 배치할 의심스러운 파일에 대한 중앙 지정입니다. 또한 선택한 파일을 전자 메일로 **Avira** 맬웨어 연구 센터에 보낼 수 있습니다.
 - 스케줄러 섹션에서는 예약된 검사 및 업데이트 작업과 백업 작업을 구성하고 기존 작업을 적용 또는 삭제할 수 있습니다.
 - 보고서 섹션에서는 수행된 작업 결과를 볼 수 있습니다.
 - 이벤트 섹션에서는 특정 프로그램 모듈에서 생성한 이벤트를 볼 수 있습니다.

4.1.2 게임 모드

컴퓨터 시스템에서 응용 프로그램을 전체 화면 모드로 실행하는 경우 게임 모드를 활성화하여 제품 메시지와 팝업 창의 데스크톱 알림을 고의적으로 일시 중지할 수 있습니다. Avira FireWall에서 구성한 정의된 모든 어댑터와 응용 프로그램 규칙이 적용되지만 네트워크 이벤트 알림과 팝업 창이 나타나지 않습니다.

설정/해제 버튼을 클릭하여 게임 모드를 사용하도록 설정하거나 자동 모드를 유지할 수 있습니다. 기본적으로 게임 모드가 **자동**으로 설정되어 녹색으로 표시됩니다. 기본적으로 이 기능은 자동으로 설정되므로 전체 화면이 필요한 응용 프로그램을 실행할 때마다 Avira 제품이 게임 모드로 자동 전환됩니다.

- ▶ 게임 모드를 활성화하려면 **해제** 버튼 왼쪽에 있는 버튼을 클릭합니다.
 - ↳ 게임 모드가 사용되고 노란색으로 표시됩니다.

참고

네트워크 이벤트 및 위협에 관한 중요한 데스크톱 알림과 경고를 받을 수 없으므로 일시적으로만 기본 설정 **해제**를 자동 전체 화면 인식 모드로 변경하는 것이 좋습니다.

4.1.3 구성

"구성"에서 Avira 제품에 대한 설정을 정의할 수 있습니다. 설치 후 Avira 제품은 컴퓨터 시스템을 최적으로 보호하기 위한 표준 설정으로 구성됩니다. 하지만 컴퓨터 시스템이나 Avira 제품에 대한 특정 요구 사항에 따라 프로그램의 보호 구성 요소를 조정해야 할 수 있습니다.



구성을 선택하면 대화 상자가 열립니다. **확인** 또는 **적용** 버튼을 통해 구성 설정을 저장하거나, 취소 버튼을 클릭하여 설정을 삭제하거나, **기본값** 버튼을 사용하여 기본 구성 설정을 복원할 수 있습니다. 왼쪽 탐색 막대에서 개별 구성 섹션을 선택할 수 있습니다.

구성 액세스

다음과 같은 방법을 사용하여 구성에 액세스할 수 있습니다.

- Windows 제어판을 통해
- Windows 보안 센터를 통해 - Windows XP 서비스 팩 2부터
- Avira 제품의 트레이 아이콘을 통해
- 제어 센터에서 메뉴 항목 기타 > 구성을 통해
- 제어 센터에서 구성 버튼을 통해

참고

제어 센터의 **구성** 버튼을 통해 구성에 액세스할 때는 제어 센터에서 활성화된 섹션의 "구성" 레지스터로 이동합니다. **고급 모드**가 활성화되어야 개별 구성 레지스터를 선택할 수 있습니다. 이 경우 고급 모드를 활성화할 것인지 묻는 대화 상자가 나타납니다.

구성 작업

Windows 탐색기에서처럼 구성 창에서 탐색합니다.

- ▶ 트리 구조의 항목을 클릭하면 세부 정보 창에 이 구성 섹션이 표시됩니다.
- ▶ 항목 앞에 있는 더하기 기호를 클릭하면 구성 섹션이 확장되고 트리 구조에 구성 하위 섹션이 표시됩니다.
- ▶ 구성 하위 섹션을 숨기려면 확장한 구성 섹션 앞에 있는 빼기 기호를 클릭합니다.

참고

구성 옵션을 활성화 또는 비활성화하고 버튼을 사용하려면 "[Alt] + 옵션 이름이나 버튼 설명에 밑줄로 표시된 문자" 키 조합을 사용할 수도 있습니다.

참고

모든 구성 섹션은 **고급 모드**에서만 표시됩니다. 모든 구성 섹션을 표시하려면 **고급 모드**를 활성화합니다. 고급 모드는 활성화 시 정의해야 하는 암호로 보호할 수 있습니다.

구성 설정을 확인하려면 다음을 수행합니다.

- ▶ **확인**을 클릭합니다.
 - ↳ 구성 창이 닫히고 설정이 적용됩니다.
 - 또는 -
- ▶ **적용**을 클릭합니다.
 - ↳ 설정이 적용됩니다. 구성 창은 열린 채로 유지됩니다.

설정을 확인하지 않고 구성을 마치려면 다음과 같이 합니다.

- ▶ **취소**를 클릭합니다.
 - ↳ 구성 창이 닫히고 설정이 취소됩니다.

모든 구성 설정을 기본값으로 복원하려면 다음과 같이 합니다.

- ▶ **기본값**을 클릭합니다.
 - ↳ 구성의 모든 설정을 기본값으로 복원합니다. 기본 설정으로 복원하면 모든 수정 사항과 사용자 지정 항목이 손실됩니다.

구성 옵션 개요


다음 구성 옵션을 사용할 수 있습니다.

- **Scanner:** 수동 검사 구성
 - 검색 시 작업
 - 압축 검사 옵션
 - 시스템 검사 예외
 - 시스템 검사 추론
 - 보고서 기능 설정
- **Real-Time Protection:** 실시간 검사 구성
 - 검사 옵션
 - 검색 시 작업
 - 추가 작업
 - 실시간 검사 예외
 - 실시간 검사 추론
 - 보고서 기능 설정
- **Backup:**
 - Backup 구성 요소 설정(증분형 백업, 백업 중 바이러스 검사)
 - 예외: 저장할 파일 정의
 - 보고서 기능 설정
- **업데이트:** 업데이트 설정 구성
 - 프록시 설정
- **FireWall:** FireWall 구성
 - 어댑터 규칙 설정
 - 사용자 정의 응용 프로그램 규칙 설정
 - 신뢰할 수 있는 공급업체 목록(응용 프로그램의 네트워크 액세스 관련 예외)
 - 확장 설정: 자동 규칙 시간 초과, Windows 방화벽 중지, 알림
 - 팝업 설정(응용 프로그램에 의한 네트워크 액세스 알림)
- **Web Protection:** Web Protection 구성
 - 검사 옵션: Web Protection 사용/사용 안 함
 - 검색 시 작업
 - 차단된 액세스: 사용자 동의 없이 설치된 파일 형식 및 MIME 형식, 알 수 없는 원치 않는 URL(맬웨어, 푸시 등)에 대한 웹 필터
 - Web Protection 검사 예외: URL, 파일 형식, MIME 형식
 - Web Protection 추론

- 보고서 기능 설정
- **Mail Protection:** Mail Protection 구성
 - 검사 옵션: POP3 계정, IMAP 계정, 보내는 전자 메일(SMTP) 모니터링 사용
 - 검색 시 작업
 - 추가 작업
 - Mail Protection 검사 추론
 - AntiBot 기능: 허용된 SMTP 서버, 허용된 전자 메일 보내는 사람
 - Mail Protection 검사 예외
 - 캐시 구성, 캐시 비우기
 - 스팸 방지 학습 데이터베이스 구성, 학습 데이터베이스 삭제
 - 보낸 전자 메일의 바닥글 구성
 - 보고서 기능 설정
- **자녀 보호:**
 - **Safe Browsing:** 인터넷 사용에 대한 역할 기반 필터와 역할 시간 제한을 사용한 자녀 보호 기능
- **일반:**
 - Scanner 및 Real-Time Protection에 대한 위협 범주
 - 고급 보호: ProActiv 및 Protection Cloud 기능을 사용할 수 있는 옵션입니다.
 - 응용 프로그램 필터: 응용 프로그램 차단 또는 허용
 - 제어 센터 및 구성 액세스에 대한 암호 보호
 - 보안: 자동 시작 차단 기능, 제품 보호, Windows 호스트 파일 보호
 - WMI: WMI 지원 사용
 - 이벤트 로그 구성
 - 보고 기능 구성
 - 사용된 디렉터리 설정
 - 맬웨어 발견 시 알림음 구성

4.1.4 트레이 아이콘

설치하면 Avira 제품의 트레이 아이콘이 작업 표시줄의 시스템 트레이에 표시됩니다.

아이콘	설명
	Avira Real-Time Protection이 실행되었으며 FireWall이 실행되었음
	Avira Real-Time Protection이 실행 중지되었거나 FireWall이 실행 중지되었음

트레이 아이콘에는 Real-Time Protection 및 FireWall 서비스의 상태가 표시됩니다.

트레이 아이콘의 상황에 맞는 메뉴를 통해 Avira 제품의 주요 기능에 빠르게 액세스할 수 있습니다. 상황에 맞는 메뉴를 열려면 마우스 오른쪽 버튼으로 트레이 아이콘을 클릭합니다.

상황에 맞는 메뉴의 항목

- **Real-Time Protection 사용:** Avira Real-Time Protection을 사용하거나 사용하지 않습니다.
- **Mail Protection 사용:** Avira Mail Protection을 사용하거나 사용하지 않습니다.
- **Web Protection 사용:** Avira Web Protection을 사용하거나 사용하지 않습니다.
- **FireWall:**
 - **FireWall 사용:** Avira FireWall을 사용하거나 사용하지 않습니다.
 - **모든 트래픽 차단:** 사용합니다. 호스트 컴퓨터 시스템(로컬 호스트/IP 127.0.0.1)으로의 전송을 제외한 모든 데이터 전송을 차단합니다.
- **Avira Internet Security 시작:** 제어 센터를 엽니다.
- **Avira Internet Security 구성:** 구성을 엽니다.
- **내 메시지:** Avira 제품에 대한 최신 정보가 있는 슬라이드업을 엽니다.
- **내 통신 설정:** 제품 메시지 구독 센터를 엽니다.
- **업데이트 시작** 업데이트를 시작합니다.
- **도움말:** 온라인 도움말을 엽니다.
- **Avira Internet Security 정보:** Avira 제품에 대한 정보(제품 정보, 버전 정보, 라이선스 정보)가 있는 대화 상자를 엽니다.
- **Avira 웹 사이트:** 인터넷의 Avira 웹 포털을 엽니다. 인터넷에 연결되어 있어야 합니다.

4.2 Avira SearchFree Toolbar

Avira SearchFree Toolbar에는 Avira SearchFree와 Toolbar의 두 가지 기본 구성 요소가 포함됩니다.

Avira SearchFree Toolbar는 추가 기능으로 설치됩니다. 브라우저에 처음 액세스하면(Firefox 및 Internet Explorer에서) Toolbar 설치 권한을 묻는 팝업이 나타납니다. Avira SearchFree Toolbar를 설치하려면 이를 승인해야 합니다.

Avira SearchFree는 검색 엔진이며 Avira 웹 사이트와 웹, 이미지 및 비디오 채널에 링크된 클릭 가능한 Avira 로고를 포함합니다. 이를 통해 Avira 사용자는 더 안전하게 인터넷을 검색할 수 있습니다.

웹 브라우저에 통합되는 toolbar는 검색 상자, Avira 웹 사이트로 연결되는 Avira 로고, 두 개의 상태 표시, 세 개의 위젯 및 **Options** 메뉴로 구성됩니다.

- **검색 Toolbar**
무료 검색 Toolbar로 Avira 검색 엔진을 사용하여 인터넷을 빠르게 검색할 수 있습니다.
- **상태 표시**
상태 표시는 Web Protection의 상태 및 Avira 제품의 최신 업데이트 상태에 대한 정보를 제공하며 PC를 보호하기 위해 취해야 하는 조치를 식별하는 데 도움을 줍니다.
- **위젯**
Avira는 가장 중요한 인터넷 관련 기능에 세 개의 위젯을 제공합니다. 클릭 한 번만으로 Facebook 및 전자 메일에 직접 액세스하거나 안전하게 웹을 탐색할 수 있습니다(Firefox 및 Internet Explorer에서만).
- **옵션**
Options 메뉴를 사용하여 toolbar 옵션에 액세스하고, 기록을 지우고, toolbar 도움말과 정보를 찾고 웹 브라우저에서 직접 Avira SearchFree Toolbar를 제거할 수 있습니다(Firefox 및 Internet Explorer에서만).

4.2.1 사용

Avira SearchFree

Avira SearchFree를 사용하여 인터넷을 탐색할 용어를 개수에 상관 없이 정의할 수 있습니다.



검색 상자에 용어를 입력하고 **Enter** 키를 누르거나 **Search**을 클릭하십시오. 그러면 Avira SearchFree 엔진이 인터넷을 검색하여 그 결과를 브라우저 창에 표시합니다.



Internet Explorer, Firefox 및 Chrome에서 Avira SearchFree를 사용자 지정하는 방법을 보려면 [옵션](#)으로 이동하십시오.

상태 표시

Web Protection

다음의 아이콘과 메시지를 사용하여 PC를 보호하기 위해 취해야 하는 조치를 식별할 수 있습니다.

아이콘	상태 표시	설명
	<i>Web Protection</i>	커서를 아이콘 위로 올리면 <i>Avira Web Protection is active. Your browsing is protected.</i> 메시지가 표시됩니다. 별도의 조치는 필요하지 않습니다.
	<i>Web Protection is inactive</i>	커서를 아이콘 위로 올리면 <i>Avira Web Protection is off. Click to find out how to turn it on.</i> 메시지가 나타납니다. → 기술 자료 문서 중 하나가 열립니다.

	No Web Protection	<p>커서를 아이콘 위로 올리면 다음 메시지 중 하나가 나타납니다.</p> <ul style="list-style-type: none"> You do not have Avira Web Protection installed. Click to find out how to protect your browsing. <p>Avira Antivirus를 올바르게 않게 설치한 경우 이 메시지가 나타납니다.</p> <ul style="list-style-type: none"> Web Protection is included for free with Avira Antivirus. Click to find out how to install it. <p>Web Protection을 설치하지 않았거나 제거한 경우에 이 메시지가 나타납니다.</p> <p>→ 두 경우 모두 Avira 제품을 다운로드할 수 있는 Avira 홈 페이지로 이동됩니다.</p>
	Error	<p>커서를 아이콘 위로 올리면 <i>Avira reported an error. Click to contact Support for help.</i> 메시지가 나타납니다.</p> <ul style="list-style-type: none"> 회색 아이콘 또는 텍스트를 클릭하면 Avira 지원 페이지로 이동합니다.

위젯

Avira SearchFree에는 최근 인터넷 탐색의 가장 중요한 기능인 Facebook, 전자 메일 및 Browser Security의 세 위젯이 포함되어 있습니다.

Facebook

이 기능을 사용하면 Facebook의 모든 최신 메시지를 받을 수 있습니다.

전자 메일

Toolbar에서 전자 메일 기호를 클릭하면 드롭다운 목록이 표시됩니다. 가장 많이 사용되는 전자 메일 공급자 중에서 선택할 수 있습니다.

Browser Security

이 위젯은 일상적으로 필요할 수 있는 모든 인터넷 보안 옵션을 원클릭으로 제공합니다. 이

옵션은 Firefox 및 Internet Explorer에만 사용할 수 있습니다. 기능의 이름은 브라우저에 따라 다를 수 있습니다.

- **팝업 차단기**

이 옵션을 활성화하면 모든 팝업 창이 차단됩니다.

- **쿠키 차단**

이 옵션을 활성화하면 쿠키가 사용자 컴퓨터에 저장되지 않습니다.

- **Private Browsing(Firefox) / InPrivate Browsing(Internet Explorer)**

서핑 중 인터넷에 어떠한 개인 정보도 남기지 않으려는 경우 이 옵션을 선택하십시오. 이 옵션은 Internet Explorer 7 및 8에만 사용할 수 있습니다.

- **최근 기록 지우기(Firefox)/검색 기록 삭제(Internet Explorer)**

이 옵션을 사용하면 인터넷 활동에 대한 모든 기록을 지울 수 있습니다.


Website Safety Advisor


Website Safety Advisor는 인터넷 검색 중 안전 등급을 제공합니다.

방문 중인 웹 사이트의 평판을 평가할 수 있으며 보안에 높거나 낮은 위험을 주는지 여부를 확인할 수 있습니다.

또한 이 위젯은 도메인 소유자, 웹 사이트가 안전하거나 위험한 것으로 등급 지정된 이유 등과 같은 웹 사이트에 대한 추가 정보도 제공합니다.

Website Safety Advisor의 상태는 Toolbar 및 검색 결과에 Avira 트레이 아이콘처럼 표시되며 다음과 같은 아이콘과 함께 표시됩니다.

아이콘	상태 표시	설명
	Safe	안전한 웹 사이트를 나타내는 녹색 체크 표시입니다.
	Low risk	낮은 위험도를 나타내는 웹 사이트에 대한 노란색 느낌표 표시입니다.
	High risk	보안에 대한 높은 위험도를 나타내는 웹 사이트에 대한 빨간색 정지 신호입니다.
	Unknown	상태를 알 수 없는 경우 회색 물음표 표시가 나타납니다.

	<i>Verifying</i>	웹 사이트의 상태를 확인 중일 때 이 기호가 나타납니다.
---	------------------	---------------------------------

Browser Tracking Blocker

Browser Tracking Blocker를 사용하면 인터넷 검색 중 추적기가 나에 대한 정보를 수집하는 것을 방지할 수 있습니다.

이 위젯을 통해 차단할 추적기와 허용할 추적기를 선택할 수 있습니다.

추적 회사는 다음 세 범주로 분류됩니다.

- 소셜 네트워크
- 광고 네트워크
- 기타 회사

4.2.2 옵션

Avira SearchFree Toolbar는 Internet Explorer, Firefox 및 Google Chrome과 호환되며 다음 세 웹 브라우저에서 구성할 수 있습니다.

- [Internet Explorer 구성 옵션](#)
- [Firefox 구성 옵션](#)
- [Google Chrome 구성 옵션](#)

Internet Explorer

Internet Explorer에서는 Avira SearchFree Toolbar에 대한 다음의 구성 옵션을 **Options** 메뉴에서 사용할 수 있습니다.

Toolbar options

Search

Avira search engine

Avira search engine 메뉴에서는 검색에 사용할 검색 엔진을 선택할 수 있습니다. 검색 엔진은 미국, 브라질, 독일, 스페인, 유럽, 프랑스, 이탈리아, 네덜란드, 러시아 및 영국에 대해 사용할 수 있습니다.

Open searches in

Open searches in 옵션 메뉴에서는 검색 결과를 현재 창, 새 창 또는 새 탭 중 어디에 표시할지를 선택할 수 있습니다.

Display recent searches

Display recent searches 옵션을 선택하면 검색 toolbar의 텍스트 입력 상자 아래에 이전 검색 용어를 표시할 수 있습니다.

Auto clear recent search history when I close the browser

이전 검색을 저장하지 않고 웹 브라우저를 닫을 때 기록을 지우려면 **Auto clear recent search history when I close the browser** 옵션을 선택하십시오.

More options

Select toolbar language

Select toolbar language에서는 Avira SearchFree Toolbar의 언어를 선택할 수 있습니다. Toolbar는 영어, 독일어, 스페인어, 프랑스어, 이탈리아어, 포르투갈어 및 네덜란드어로 사용할 수 있습니다.

참고

가능한 경우 Avira SearchFree Toolbar의 기본 언어는 프로그램의 언어에 해당합니다. Toolbar를 현재 국가의 언어로 사용할 수 없는 경우의 기본 언어는 영어입니다.

Show button text labels

Avira SearchFree Toolbar 아이콘 옆의 텍스트를 숨기려면 **Show button text labels** 옵션을 해제하십시오.

Clear history

이전 검색을 저장하지 않고 기록을 즉시 지우려면 **Clear history** 옵션을 선택하십시오.

Help

Toolbar에 관련된 자주 묻는 질문(FAQ)이 포함된 웹 사이트에 액세스하려면 **Help**를 클릭하십시오.

Uninstall

Avira SearchFree Toolbar를 Internet Explorer에서 직접 제거할 수도 있습니다([웹 브라우저를 통해 제거](#)).

About

About를 클릭하면 설치된 Avira SearchFree Toolbar의 버전이 표시됩니다.

Firefox

Firefox 웹 브라우저에서는 Avira SearchFree Toolbar에 대한 다음의 구성 옵션을 **Options** 메뉴에서 사용할 수 있습니다.

Toolbar options

Search

Select Avira search engine

Avira search engine 메뉴에서는 검색에 사용할 검색 엔진을 선택할 수 있습니다. 검색 엔진은 미국, 브라질, 독일, 스페인, 유럽, 프랑스, 이탈리아, 네덜란드, 러시아 및 영국에 대해 사용할 수 있습니다.

Display recent searches

Display recent searches 옵션을 선택하면 검색 도구 모음의 화살표를 클릭하여 이전 검색 용어를 표시할 수 있습니다. 검색 결과를 다시 표시하려면 용어를 선택하십시오.

Auto clear recent search history when I close the browser

이전 검색을 저장하지 않고 웹 브라우저를 닫을 때 기록을 지우려면 **Auto clear recent search history when I close the browser** 옵션을 선택하십시오.

Display Avira search results when I type keywords or invalid URLs into the browser address bar

이 옵션을 선택하면 브라우저의 주소 표시줄에 키워드 또는 유효하지 않은 URL을 입력할 때마다 검색이 시작되어 검색 결과가 표시됩니다.

More options

Select toolbar language

Select toolbar language에서는 Avira SearchFree Toolbar의 언어를 선택할 수 있습니다. Toolbar는 영어, 독일어, 스페인어, 프랑스어, 이탈리아어, 포르투갈어 및 네덜란드어로 사용할 수 있습니다.

참고

가능한 경우 Avira SearchFree Toolbar의 기본 언어는 프로그램의 언어에 해당합니다. Toolbar를 현재 국가의 언어로 사용할 수 없는 경우의 기본 언어는 영어입니다.

Show button text labels

Avira SearchFree Toolbar 아이콘 옆의 텍스트를 숨기려면 **Show button text labels** 옵션을 해제하십시오.

Clear history

이전 검색을 저장하지 않고 기록을 즉시 지우려면 **Clear history** 옵션을 선택하십시오.

Help

Toolbar에 관련된 자주 묻는 질문(FAQ)이 포함된 웹 사이트에 액세스하려면 **Help**를 클릭하십시오.

Uninstall

Avira SearchFree Toolbar를 Firefox에서 직접 제거할 수도 있습니다([웹 브라우저를 통해 제거](#)).

About

About를 클릭하면 설치된 Avira SearchFree Toolbar의 버전이 표시됩니다.

Google Chrome

Chrome 웹 브라우저에서는 빨간색 Avira 우산 메뉴 아래에서 Avira SearchFree Toolbar에 대한 다음의 구성 옵션을 사용할 수 있습니다.

Help

Toolbar에 관련된 자주 묻는 질문(FAQ)이 포함된 웹 사이트에 액세스하려면 **Help**를 클릭하십시오.

제거 지침

도구 모음을 제거하는 데 필요한 모든 정보가 포함된 기사로 연결됩니다.

About

About를 클릭하면 설치된 Avira SearchFree Toolbar의 버전이 표시됩니다.

Avira SearchFree Toolbar 표시/숨기기

여기를 클릭하면 웹 브라우저에서 Avira SearchFree Toolbar를 숨기거나 표시할 수 있습니다.

4.2.3 제거

Avira SearchFree Toolbar를 제거하려면(예를 들어 Windows 7에서):

- ▶ Windows 시작 메뉴에서 **제어판**을 엽니다.

- ▶ 프로그램 및 기능을 더블클릭합니다.
- ▶ 목록에서 **Avira SearchFree Toolbar plus Web Protection**을 선택하고 제거를 클릭합니다.
 - ↳ 이 제품을 제거할 것인지 확인하는 메시지가 표시됩니다.
- ▶ 예를 클릭하여 확인합니다.
 - ↳ Avira SearchFree Toolbar plus Web Protection이 제거되고 컴퓨터가 다시 시작될 때 Avira SearchFree Toolbar plus Web Protection의 모든 디렉터리, 파일 및 레지스트리 항목이 삭제됩니다.

웹 브라우저를 통한 제거

Avira SearchFree Toolbar를 브라우저에서 직접 제거할 수도 있습니다. 이 옵션은 **Firefox** 및 **Internet Explorer**에서만 사용할 수 있습니다.

- ▶ 검색 toolbar에서 **Options** 메뉴를 엽니다.
- ▶ **Uninstall**를 클릭합니다.
 - ↳ 웹 브라우저가 열려 있으면 이를 닫으라는 메시지가 나타납니다.
- ▶ 웹 브라우저를 닫고 **확인**을 클릭합니다.
 - ↳ Avira SearchFree Toolbar plus Web Protection이 제거되고 컴퓨터가 다시 시작될 때 Avira SearchFree Toolbar plus Web Protection의 모든 디렉터리, 파일 및 레지스트리 항목이 삭제됩니다.

참고

Avira SearchFree Toolbar를 제거하려면 부가 기능 관리자에서 toolbar를 활성화해야 합니다.

부가 기능으로 제거

Toolbar는 부가 기능으로 설치되기 때문에 부가 기능 제거로 제거할 수 있습니다.

Firefox

┆ > **Add-ons > Extensions**을 클릭합니다. 여기에서 Avira 부가 기능을 관리할 수 있습니다. 즉 도구 모음을 활성화하거나 비활성화하고 제거할 수 있습니다.

Internet Explorer

추가 기능 관리 > 도구 모음 및 확장으로 이동합니다. 여기에서는 Avira SearchFree Toolbar를 활성화 및 비활성화하거나 제거할 수 있습니다.

Google Chrome

옵션 > 확장을 클릭하여 Toolbar를 활성화/비활성화하거나 제거합니다.

4.3 방법

"방법" 장은 Avira 제품의 가장 중요한 기능에 대한 정보뿐만 아니라 라이선스 및 제품 활성화에 대한 간단한 지침을 제공합니다. 선택한 짧은 문서는 Avira 제품의 기능에 대한 개요로 제공됩니다. 이러한 문서가 이 도움말 센터의 각 섹션에 있는 세부 정보를 대체하지는 않습니다.

4.3.1 라이선스 활성화

Avira 제품의 라이선스를 활성화하려면:

.KEY 라이선스 파일을 사용하여 Avira 제품의 라이선스를 활성화합니다. 라이선스 파일은 Avira에서 전자 메일로 보내드립니다. 라이선스 파일에는 하나의 주문 프로세스에서 주문한 모든 제품의 라이선스가 포함되어 있습니다.

Avira 제품을 아직 설치하지 않은 경우:

- ▶ 컴퓨터의 로컬 디렉터리에 라이선스 파일을 저장합니다.
- ▶ Avira 제품을 설치합니다.
- ▶ 설치 중에 라이선스 파일의 저장 위치를 입력합니다.

Avira 제품을 이미 설치한 경우:

- ▶ 파일 관리자 또는 활성화 전자 메일에서 라이선스 파일을 더블클릭한 다음 라이선스 관리자가 열리면 화면의 지침대로 수행합니다.

- 또는 -

Avira 제품의 제어 센터에서 메뉴 항목 **도움말 > 라이선스 관리**를 선택합니다.

참고

Windows Vista에서는 사용자 계정 컨트롤 대화 상자가 나타납니다. 관리자로 로그인합니다. **계속**을 클릭합니다.

- ▶ 라이선스 파일을 강조 표시하고 **열기**를 클릭합니다.
 - ↳ 메시지가 나타납니다.
- ▶ **확인**을 클릭하여 확인합니다.

→ 라이선스가 활성화되었습니다.

- ▶ 필요한 경우 시스템을 다시 시작합니다.

4.3.2 제품 정품 인증

Avira 제품을 정품 인증하려면 다음 옵션을 선택할 수 있습니다.

유효한 정식 라이선스를 사용한 정품 인증

정식 라이선스로 프로그램의 정품 인증을 받으려면, 구매한 라이선스에 대한 데이터가 포함된 유효한 정품 인증 코드가 필요합니다. 정품 인증 코드는 전자 메일로 전송되거나 제품 포장재에 인쇄되어 있습니다.

평가판 라이선스를 사용한 정품 인증

Avira 제품은 자동 생성되는 평가판 라이선스로 정품 인증되며, 이 경우 한시적으로 Avira 제품의 모든 기능을 시험 사용할 수 있습니다.

참고

정품 인증하거나 평가판 라이선스를 사용하려면 활성화된 인터넷 링크가 필요합니다.

Avira의 서버에 연결할 수 없는 경우에는 사용하는 방화벽의 설정을 확인하십시오. 제품 정품 인증에는 HTTP 프로토콜과 포트 80(웹 통신) 및 암호화 프로토콜 SSL과 포트 443을 통한 통신이 사용됩니다. FireWall에서 들어오거나 나가는 데이터를 차단하지 않는지 확인하십시오. 먼저 웹 브라우저로 웹 페이지에 액세스할 수 있는지 확인하십시오.

다음은 Avira 제품을 정품 인증하는 방법입니다.

Avira 제품을 아직 설치하지 않은 경우:


- ▶ Avira 제품을 설치합니다.
 - 설치 과정에서 정품 인증 옵션을 선택하라는 메시지가 표시됩니다.
- **제품 정품 인증:** 유효한 정식 라이선스를 사용하여 정품 인증
- **테스트 제품:** 평가판 라이선스를 사용하여 정품 인증
- ▶ 정식 라이선스로 정품 인증하려면 정품 인증 코드를 입력합니다.
- ▶ 다음을 클릭하여 정품 인증 절차의 선택 항목을 확인합니다.
- ▶ 등록에 필요한 개인 데이터를 입력하고 다음을 클릭하여 확인합니다.
 - 라이선스 데이터가 다음 창에 표시됩니다. 이제 Avira 제품이 활성화되었습니다.
- ▶ 설치를 계속합니다.

Avira 제품을 이미 설치한 경우:

- ▶ 제어 센터에서 메뉴 항목 **도움말 > 라이선스 관리**를 선택합니다.
 - ↳ 정품 인증 옵션을 선택할 수 있는 *라이선스 마법사*가 열립니다. 정품 인증의 나머지 단계는 위에서 설명한 절차와 동일합니다.

4.3.3 자동 업데이트 수행

Avira 스케줄러에서 Avira 제품을 자동으로 업데이트하는 작업을 만들려면:

- ▶ 제어 센터에서 **관리 > 스케줄러** 섹션을 선택합니다.
- ▶  **새 작업 삽입** 아이콘을 클릭합니다.
 - ↳ **작업의 이름 및 설명** 대화 상자가 나타납니다.
- ▶ 작업 이름과 적절한 경우 설명을 입력합니다.
- ▶ 다음을 클릭합니다.
 - ↳ **작업 유형** 대화 상자가 나타납니다.
- ▶ 목록에서 **업데이트** 작업을 선택합니다.
- ▶ 다음을 클릭합니다.
 - ↳ **작업 시간** 대화 상자가 나타납니다.
- ▶ 업데이트 시간을 선택합니다.
 - 즉시
 - 매일
 - 매주
 - 간격
 - 단일
 - 로그인


참고


자동 업데이트를 정기적으로 수행하는 것이 좋습니다. 권장 업데이트 간격은 2시간입니다.


- ▶ 선택 항목에 따라 날짜를 지정합니다.
- ▶ 다음 추가 옵션을 선택합니다. 선택 가능 여부는 작업 유형에 따라 다릅니다.
 - **시간이 만료된 경우 작업 반복**
컴퓨터 전원이 꺼지는 등의 이유로 인해 필요한 때 수행할 수 없었던 지난 작업을 수행합니다.


- 인터넷에 연결(전화 접속)되었을 때 작업 시작
정의된 빈도 이외에, 인터넷 연결이 설정되었을 때 작업을 수행합니다.
- ▶ 다음을 클릭합니다.
 - ↳ 디스플레이 모드 선택 대화 상자가 나타납니다.
- ▶ 작업 창의 디스플레이 모드를 선택합니다.
- 표시하지 않음: 작업을 표시하지 않습니다.
- 최소화: 진행률 표시줄만 표시합니다.
- 최대화: 작업 창 전체를 표시합니다.
- ▶ 마침을 클릭합니다.
 - ↳ 새로 만든 작업이 상태가 활성화되어(체크 표시) 관리 > 스케줄러 섹션의 시작 페이지에 나타납니다.
- ▶ 필요한 경우 수행하지 않을 작업은 비활성화합니다.


작업을 더 자세히 정의하려면 다음 아이콘을 사용합니다.

 작업의 속성 보기

 작업 편집

 작업 삭제

 작업 시작

 작업 중지

4.3.4 수동 업데이트 시작

업데이트를 수동으로 시작하기 위한 다양한 옵션이 제공되며, 업데이트를 수동으로 시작한 경우에는 바이러스 정의 파일과 검사 엔진은 항상 업데이트됩니다. 제품 업데이트는 PC 보호 > 업데이트 > 제품 업데이트의 구성에서 자동으로 제품 업데이트 다운로드 및 설치 옵션을 선택한 경우에만 수행됩니다.

Avira 제품의 업데이트를 수동으로 시작하려면:

- ▶ 작업 표시줄에서 Avira 트레이 아이콘을 마우스 오른쪽 단추로 클릭합니다.
 - ↳ 그러면 상황에 맞는 메뉴가 나타납니다.
- ▶ 업데이트 시작을 선택합니다.

→ 업데이트 프로그램 대화 상자가 나타납니다.

- 또는 -

- ▶ 제어 센터에서 상태를 선택합니다.
- ▶ 최신 업데이트 필드에서 업데이트 시작 링크를 클릭합니다.
- 업데이트 프로그램 대화 상자가 나타납니다.

- 또는 -

- ▶ 제어 센터의 업데이트 메뉴에서 업데이트 시작 메뉴 명령을 선택합니다.
- 업데이트 프로그램 대화 상자가 나타납니다.

참고

자동 업데이트를 정기적으로 수행하는 것이 좋습니다. 권장 업데이트 간격은 2시간입니다.

참고

또한 Windows 보안 센터를 통해 직접 수동 업데이트를 수행할 수도 있습니다.

4.3.5 검사 프로필을 사용한 바이러스 및 맬웨어 검사

검사 프로필은 검사할 드라이브 및 디렉터리의 집합입니다.

검사 프로필을 사용하는 검사에 다음 옵션을 사용할 수 있습니다.

미리 정의된 검사 프로필 사용

미리 정의된 검사 프로필이 요구 사항과 일치하는 경우에 사용합니다.

검사 프로필을 사용자 지정하고 적용(수동 선택)

사용자 지정된 검사 프로필로 검사하려는 경우에 사용합니다.

새 검사 프로필을 만들어 적용

검사 프로필을 직접 만들려는 경우에 사용합니다.

운영 체제에 따라 다양한 아이콘을 사용하여 검사 프로필을 시작할 수 있습니다.



- Windows XP:





이 아이콘은 검사 프로필을 통해 검사를 시작합니다.

- Windows Vista:

Microsoft Windows Vista의 경우 현재로서는 제어 센터의 권한이 제한적입니다(예: 디렉터리 및 파일에 대한 액세스). 특정 작업 및 파일 액세스는 확장된 관리자 권한으로 제어 센터에서만 수행할 수 있습니다. 이 확장된 관리자 권한은 검사를 시작할 때마다 검사 프로필을 통해 부여해야 합니다.

-  이 아이콘은 검사 프로필을 통해 제한적인 검사를 시작합니다. Windows Vista에서 액세스 권한을 부여한 디렉터리 및 파일만 검사합니다.
-  이 아이콘은 확장된 관리 권한으로 검사를 시작합니다. 확인하면 선택한 검사 프로필의 모든 디렉터리 및 파일을 검사합니다.



검사 프로필을 사용하여 바이러스 및 맬웨어를 검사하려면

- ▶ 제어 센터로 이동하여 **PC 보호 > System Scanner** 섹션을 선택합니다.
 - ↳ 미리 정의된 검사 프로필이 나타납니다.
- ▶ 미리 정의된 검사 프로필 중 하나를 선택합니다.
 - 또는-
 - 검사 프로필 수동 선택을 변경합니다.
 - 또는-
 - 새 검사 프로필 만들기
- ▶ 아이콘(Windows XP:  또는 Windows Vista: )을 클릭합니다.
- ▶ **Luke Filewalker** 창이 나타나고 시스템 검사가 시작됩니다.
 - ↳ 검사가 끝나면 그 결과가 표시됩니다.

검사 프로필을 변경하려는 경우:

- ▶ 검사 프로필에서 수동 선택 파일 트리를 확장하여 검사하려는 모든 드라이브 및 디렉터리를 엽니다.
 - + 아이콘 클릭: 다음 디렉터리 수준이 표시됩니다.
 - - 아이콘 클릭: 다음 디렉터리 수준이 숨겨집니다.
- ▶ 적절한 디렉터리 수준의 관련 상자를 클릭하여 검사하려는 노드 및 디렉터리를 강조 표시합니다.
 - 디렉터리를 선택할 때 다음 옵션을 사용할 수 있습니다.
 - 하위 디렉터리를 포함한 디렉터리(검정색 확인 표시)
 - 한 디렉터리의 하위 디렉터리만 선택(회색 확인 표시, 하위 디렉터리는 검정색 확인 표시)
 - 디렉터리 선택 안 함(확인 표시 없음)

새 검사 프로필을 만들려는 경우:

- ▶  새 프로필 만들기 아이콘을 클릭합니다.
 - ↳ 이전에 만든 프로필 아래에 새 프로필이 나타납니다.
- ▶ 필요한 경우  아이콘을 클릭하여 검사 프로필의 이름을 바꿉니다.
- ▶ 각 디렉터리 수준의 확인란을 클릭하여 저장할 노드 및 디렉터리를 강조 표시합니다.
 - 디렉터리를 선택할 때 다음 옵션을 사용할 수 있습니다.
 - 하위 디렉터리를 포함한 디렉터리(검정색 확인 표시)
 - 한 디렉터리의 하위 디렉터리만 선택(회색 확인 표시, 하위 디렉터리는 검정색 확인 표시)
 - 디렉터리 선택 안 함(확인 표시 없음)

4.3.6 끌어서 놓기를 사용한 바이러스 및 맬웨어 검사

끌어서 놓기를 사용하여 바이러스 및 맬웨어를 체계적으로 검사하려면:

- ✓ Avira 제품의 제어 센터가 열려 있습니다.
- ▶ 검사하려는 파일 또는 디렉터리를 강조 표시합니다.
- ▶ 마우스 왼쪽 단추를 사용하여 강조 표시된 파일 또는 디렉터리를 제어 센터로 끌어옵니다.
 - ↳ **Luke Filewalker** 창이 나타나고 시스템 검사가 시작됩니다.
 - ↳ 검사가 끝나면 그 결과가 표시됩니다.

4.3.7 상황에 맞는 메뉴를 사용한 바이러스 및 맬웨어 검사

상황에 맞는 메뉴를 사용하여 바이러스 및 맬웨어를 체계적으로 검사하려면:


- ▶ 검사하려는 파일 또는 디렉터리를 Windows 탐색기, 바탕 화면 또는 열려 있는 Windows 디렉터리에서처럼 마우스 오른쪽 버튼으로 클릭합니다.
 - ↳ Windows 탐색기의 상황에 맞는 메뉴가 나타납니다.
- ▶ 상황에 맞는 메뉴에서 **Avira**를 사용하여 선택한 파일 검사를 선택합니다.
 - ↳ **Luke Filewalker** 창이 나타나고 시스템 검사가 시작됩니다.
 - ↳ 검사가 끝나면 그 결과가 표시됩니다.

4.3.8 바이러스 및 맬웨어 자동 검사

참고

설치 후에는 검사 작업 **전체 시스템 검사**가 스케줄러에 생성되어, 전체 시스템 검사가 권장 간격에 따라 자동으로 수행됩니다.

바이러스 및 맬웨어를 자동 검사하는 작업을 만들려면:


- ▶ 제어 센터에서 **관리 > 스케줄러** 섹션을 선택합니다.
- ▶  아이콘을 클릭합니다.
 - ↳ **작업의 이름 및 설명** 대화 상자가 나타납니다.
- ▶ 작업 이름과 적절한 경우 설명을 입력합니다.
- ▶ 다음을 클릭합니다.
 - ↳ **작업 유형** 대화 상자가 나타납니다.
- ▶ **검사 작업**을 선택합니다.
- ▶ 다음을 클릭합니다.
 - ↳ **프로필 선택** 대화 상자가 나타납니다.
- ▶ 검사할 프로필을 선택합니다.
- ▶ 다음을 클릭합니다.
 - ↳ **작업 시간** 대화 상자가 나타납니다.
- ▶ 검사 시간을 선택합니다.
 - 즉시
 - 매일
 - 매주
 - 간격
 - 단일
 - 로그인
- ▶ 선택 항목에 따라 날짜를 지정합니다.
- ▶ 다음 추가 옵션을 선택합니다. 선택 가능 여부는 작업 유형에 따라 다릅니다.
 - 시간이 만료된 경우 작업 반복


컴퓨터 전원이 꺼지는 등의 이유로 인해 필요할 때 수행할 수 없었던 지난 작업을 수행합니다.
- ▶ 다음을 클릭합니다.


↳ 디스플레이 모드 선택 대화 상자가 나타납니다.


- ▶ 작업 창의 디스플레이 모드를 선택합니다.
- **표시하지 않음**: 작업을 표시하지 않습니다.
- **최소화**: 진행률 표시줄만
- **최대화**: 전체 작업 창
- ▶ 검사가 완료된 경우 컴퓨터를 자동으로 종료하려면 **작업이 완료되면 컴퓨터 종료** 옵션을 선택합니다. 이 옵션은 디스플레이 모드가 최소화 또는 최대화로 설정된 경우에만 사용할 수 있습니다.
- ▶ **마침**을 클릭합니다.
 - ↳ 새로 만든 작업이 상태가 활성화되어(체크 표시) **관리 > 스케줄러** 섹션의 시작 페이지에 나타납니다.
- ▶ 필요한 경우 수행하지 않을 작업은 비활성화합니다.


작업을 더 자세히 정의하려면 다음 아이콘을 사용합니다.

 작업의 속성 보기

 작업 편집

 작업 삭제

 작업 시작



 작업 중지

4.3.9 Rootkits 및 활성 맬웨어에 대한 대상 지정 검사

활성 rootkits을 검사하려면 미리 정의된 검사 프로파일인 **rootkits 및 활성 맬웨어 검사**를 사용합니다.

활성 rootkits을 체계적으로 검사하려면:

- ▶ 제어 센터로 이동하여 **PC 보호 > Scanner** 섹션을 선택합니다.
 - ↳ 미리 정의된 검사 프로파일이 나타납니다.
- ▶ 미리 정의된 검사 프로파일 **rootkits 및 활성 맬웨어 검사**를 선택합니다.
- ▶ 필요한 경우 디렉터리 수준의 체크박스를 클릭하여 검사할 다른 노드 및 디렉터리를 강조 표시합니다.

- ▶ 아이콘(Windows XP:  또는 Windows Vista: )을 클릭합니다.
 - ↳ **Luke Filewalker** 창이 나타나고 시스템 검사가 시작됩니다.
 - ↳ 검사가 끝나면 그 결과가 표시됩니다.

4.3.10 검색한 바이러스 및 맬웨어에 대응

Avira 제품의 개별 보호 구성 요소별로 Avira 제품에서 검색된 바이러스 또는 사용자 동의 없이 설치된 프로그램에 대응하는 방법을 정의할 수 있습니다. 구성의 검색 시 작업에서 정의합니다.

Real-Time Protection의 ProActiv에 대한 구성 가능한 작업 옵션은 없습니다. 검색 알림은 항상 **Real-Time Protection: 의심스러운 응용 프로그램 동작** 창에서 제공됩니다.

Scanner에 대한 작업 옵션

대화형

대화형 작업 모드에서 Scanner의 검사 결과가 대화 상자에 표시됩니다. 이 옵션은 기본 설정으로 선택됩니다.

Scanner 검사의 경우 검사가 완료되면 영향받는 파일 목록과 함께 알림이 제공됩니다. 콘텐츠별 메뉴를 사용하여 감염된 여러 파일에 대해 실행할 작업을 선택할 수 있습니다. 감염된 모든 파일에 대해 표준 작업을 실행하거나 Scanner를 취소할 수 있습니다.

자동

자동 작업 모드에서는 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견되면 여기서 선택한 작업이 자동으로 실행됩니다.

Real-Time Protection에 대한 작업 옵션:

대화형

대화형 작업 모드에서는 데이터 액세스가 거부되고 데스크톱 알림이 표시됩니다. 데스크톱 알림에서는 검색된 맬웨어를 제거하거나 **자세히** 버튼을 사용하여 추가 바이러스 관리를 위해 Scanner 구성 요소로 맬웨어를 전달할 수 있습니다. Scanner는 검색 알림과 함께 상황에 맞는 메뉴를 통해 영향받는 파일을 관리할 수 있는 다양한 옵션이 포함된 창을 표시합니다. 검색 > Scanner를 참조하십시오.

자동

자동 작업 모드에서는 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견되면 여기서 선택한 작업이 자동으로 실행됩니다.

Mail Protection, Web Protection에 대한 작업 옵션:

대화형

대화형 작업 모드에서는 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견되면 감염된 개체에 대해 수행할 작업을 선택할 수 있는 대화 상자가 나타납니다. 이 옵션은 기본 설정으로 선택됩니다.

자동

자동 작업 모드에서는 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견되면 여기서 선택한 작업이 자동으로 실행됩니다.

대화형 작업 모드에서는 알림에 표시된 감염된 개체에 대한 작업을 선택하고 **확인**을 클릭하여 그 작업을 실행하는 방법으로, 감염된 바이러스 및 사용자 동의 없이 설치된 프로그램에 대응할 수 있습니다.

감염된 개체 처리를 위한 다음 작업을 선택할 수 있습니다.

참고

운영 체제, 검색을 보고하는 보호 구성 요소(Avira Real-Time Protection, Avira Scanner, Avira Mail Protection, Avira Web Protection) 및 검색된 맬웨어 유형에 따라 선택할 수 있는 옵션이 달라집니다.

Scanner 및 Real-Time Protection에 대한 작업(ProActiv 검색 제외):

복구

파일이 복구됩니다.

이 옵션은 감염된 파일이 복구 가능한 경우에만 사용할 수 있습니다.

이름 바꾸기

파일 이름의 확장명이 ***.vir**로 바뀝니다. 따라서 더블클릭과 같은 방법으로 이러한 파일에 더 이상 직접 액세스할 수 없습니다. 파일을 나중에 복구하고 원래 이름을 다시 지정할 수 있습니다.

격리 저장소

파일이 특수한 형식(***.qua**)으로 패키징되어 하드 디스크에 있는 격리 저장소 디렉터리 **INFECTED**로 이동합니다. 따라서 더 이상 직접 액세스할 수 없습니다. 이 디렉터리의 파일은 나중에 격리 저장소에서 복구하거나 필요할 경우 **Avira**로 전송할 수 있습니다.

삭제

파일이 삭제됩니다. 이 프로세스는 덮어쓰기 및 삭제보다 훨씬 빠릅니다. 부트 섹터 바이러스가 검색된 경우 부트 섹터를 삭제하는 방법으로 이를 삭제할 수 있습니다. 새 부트 섹터가 작성됩니다.

무시

추가 작업이 수행되지 않습니다. 감염된 파일은 해당 컴퓨터에서 활성 상태를 유지합니다.

덮어쓰기 및 삭제

파일을 기본 템플릿으로 덮어쓴 다음 삭제합니다. 이 파일은 복원할 수 없습니다.

경고

이 경우 데이터가 손실되고 운영 체제가 손상될 수 있습니다! 예외적인 경우에만 무시 옵션을 선택하십시오.

항상 무시

Real-Time Protection 검색 시 작업 옵션: **Real-Time Protection**에서 추가 작업을 수행하지 않습니다. 파일에 대한 액세스가 허용됩니다. 컴퓨터를 다시 시작하거나 바이러스 정의 파일을 업데이트할 때까지 추가 알림이 제공되지 않으며 이 파일에 대한 모든 추후 액세스가 허용됩니다.

격리 저장소로 복사

Rootkits 검색 시 작업 옵션: 발견된 항목이 격리 저장소로 복사됩니다.

부트 섹터 복구 | 복구 도구 다운로드

감염된 부트 섹터가 검색되는 경우 작업 옵션: 감염된 디스켓 드라이브를 복구하는 데 여러 가지 옵션을 사용할 수 있습니다. **Avira** 제품에서 복구를 수행할 수 없는 경우 부트 섹터 바이러스를 검색 및 제거하는 특수 도구를 다운로드할 수 있습니다.

참고

실행 중인 프로세스에 대해 작업을 수행하면 작업이 수행되기 전에 해당 프로세스가 종료됩니다.

ProActiv 구성 요소에서 수행하는 검색에 대한 **Real-Time Protection** 작업(응용 프로그램의 의심스러운 작업 알림):

신뢰할 수 있는 프로그램

응용 프로그램이 계속 실행되며 허용된 응용 프로그램 목록에 추가되고 **ProActiv** 구성 요소의 모니터링 대상에서 제외됩니다. 허용된 응용 프로그램 목록에 추가되면 모니터링 유형이 콘텐츠로 설정됩니다. 허용된 응용 프로그램 목록에 추가되면 모니터링 유형이 **콘텐츠**로 설정됩니다. 즉, 콘텐츠가 변경되지 않은 상태로 유지되는 경우에만 **ProActiv** 구성 요소의 모니터링 대상에서 해당 응용 프로그램이 제외됩니다. **응용 프로그램 필터: 허용된 응용 프로그램**을 참조하십시오.

프로그램 한 번 차단

응용 프로그램 차단(종료)되고 **ProActiv** 구성 요소에서 응용 프로그램 작업을 계속 모니터링합니다.

이 프로그램 항상 차단

응용 프로그램 차단(종료)되고 차단된 응용 프로그램 목록에 추가되며 더 이상 실행할 수 없습니다. **응용 프로그램 필터: 차단할 응용 프로그램**을 참조하십시오.

무시

응용 프로그램이 계속 실행되며 허용된 응용 프로그램 목록에 추가되고 **ProActiv** 구성 요소의 모니터링 대상에서 제외됩니다. **ProActiv** 구성 요소에서 응용 프로그램 작업을 계속 모니터링합니다.

Mail Protection 작업: 받는 전자 메일

격리 저장소로 이동

전자 메일과 모든 첨부 파일을 격리 저장소로 이동합니다. 영향받는 전자 메일이 삭제됩니다. 전자 메일의 텍스트 본문 및 모든 첨부 파일은 **기본 텍스트**로 바꿉니다.

메일 삭제

영향받는 전자 메일이 삭제됩니다. 전자 메일의 텍스트 본문 및 모든 첨부 파일은 **기본 텍스트**로 바꿉니다.

첨부 파일 삭제

감염된 첨부 파일이 **기본 텍스트**로 바꿉니다. 전자 메일 본문이 영향받은 경우 본문이 삭제되고 **기본 텍스트**로 바꿉니다. 전자 메일 자체는 배달됩니다.

첨부 파일을 격리 저장소로 이동

감염된 첨부 파일을 격리 저장소로 이동하고 삭제합니다(**기본 텍스트**로 바꿈). 전자 메일 본문은 배달됩니다. 영향받는 첨부 파일은 나중에 격리 관리자를 통해 배달할 수 있습니다.

무시

해당 전자 메일이 배달됩니다.

경고

따라서 바이러스 및 사용자 동의 없이 설치된 프로그램이 사용자의 컴퓨터 시스템에 액세스할 수 있습니다. 예외적인 경우에만 **무시** 옵션을 선택하십시오. 메일 클라이언트의 미리 보기를 사용하지 않도록 설정하고 절대 첨부 파일을 더블클릭하여 열지 마십시오!

Mail Protection 작업: 보내는 전자 메일

메일을 격리 저장소로 이동(보내지 않음)

전자 메일과 모든 첨부 파일을 격리 저장소로 복사하며 보내지는 않습니다. 전자 메일은 전자 메일 클라이언트의 보낸 편지함에 남아 있습니다. 전자 메일 프로그램에 오류 메시지가 표시됩니다. 사용자의 전자 메일 계정에서 보낸 다른 모든 전자 메일을 대상으로 맬웨어를 검사합니다.

메일 보내기 차단(보내지 않음)

전자 메일이 전송되지 않고 전자 메일 클라이언트의 보낸 편지함에 유지됩니다. 전자 메일 프로그램에 오류 메시지가 표시됩니다. 사용자의 전자 메일 계정에서 보낸 다른 모든 전자 메일을 대상으로 맬웨어를 검사합니다.

무시

해당 전자 메일을 보냅니다.

경고

바이러스 및 사용자 동의 없이 설치된 프로그램이 이러한 방법으로 전자 메일을 받는 사람의 컴퓨터 시스템에 침입할 수 있습니다.

Web Protection 작업:

액세스 거부

웹 서버에서 요청한 웹 사이트 및/또는 전송된 모든 데이터나 파일이 사용자의 웹 브라우저로 전송되지 않습니다. 액세스가 거부되었음을 알리는 오류 메시지가 웹 브라우저에 표시됩니다.

격리 저장소로 이동

웹 서버에서 요청한 웹 사이트 및/또는 전송된 모든 데이터나 파일을 격리 저장소로 옮깁니다. 영향받는 파일이 정보가 포함된 중요한 파일인 경우 격리 관리자를 통해 복구하거나 필요한 경우 Avira 맬웨어 연구 센터로 보낼 수 있습니다.

무시

웹 서버에서 요청한 웹 사이트 및/또는 전송된 데이터와 파일을 Web Protection이 사용자의 웹 브라우저로 전달합니다.

경고

따라서 바이러스 및 사용자 동의 없이 설치된 프로그램이 사용자의 컴퓨터 시스템에 액세스할 수 있습니다. 예외적인 경우에만 무시 옵션을 선택하십시오.

참고

복구할 수 없는 의심스러운 파일은 모두 격리 저장소로 이동하는 것이 좋습니다.

참고

또한 추론에서 보고한 파일을 Avira에 보내 분석할 수도 있습니다.

예를 들면 이러한 파일을 Avira 웹 사이트 <http://www.avira.kr/sample-upload>에 업로드할 수 있습니다.


파일 이름 앞에 붙은 *HEUR*/ 또는 *HEURISTIC*/ 접두사를 통해 추론에서 보고된 파일을 식별할 수 있습니다(예: *HEUR/testfile.**).

4.3.11 격리된 파일(*.qua) 처리

격리된 파일을 처리하려면


- ▶ 제어 센터에서 *관리* > *격리 저장소* 섹션을 선택합니다.
- ▶ 필요한 경우 원래의 파일을 다른 위치에서 해당 컴퓨터로 다시 로드할 수 있도록 해당 파일을 선택합니다.

파일에 대한 자세한 정보를 보려는 경우


- ▶ 파일을 강조 표시하고  을 클릭합니다.
 - ↳ 파일에 대한 자세한 정보가 표시되는 **속성** 대화 상자가 나타납니다.

파일을 다시 검사하려는 경우


Avira 제품의 바이러스 정의 파일이 업데이트되었고 오진 보고가 의심될 경우 파일을 검사하는 것이 좋습니다. 그러면 다시 검사하여 오진을 확인하고 파일을 복원할 수 있습니다.

- ▶ 파일을 강조 표시하고  을 클릭합니다.
 - ↳ 시스템 검사 설정을 사용하여 파일에서 바이러스 및 맬웨어를 검사합니다.
 - ↳ 검사가 끝나면 **다시 검사 통계** 대화 상자가 나타나 다시 검사하기 전과 후의 파일 상태에 대한 통계 정보를 표시합니다.

파일을 삭제하려면

- ▶ 파일을 강조 표시하고  을 클릭합니다.
- ▶ **예**를 선택하여 선택을 확인해야 합니다.

분석을 위해 Avira 맬웨어 연구 센터 웹 서버로 파일을 업로드하려는 경우

- ▶ 업로드할 파일을 강조 표시합니다.
- ▶  을 클릭합니다.
 - ↳ 대화 상자가 열리고 연락처 데이터를 입력하는 양식이 표시됩니다.
- ▶ 필요한 데이터를 모두 입력합니다.
- ▶ 유형(**의심스러운 파일** 또는 **오진 의심**)을 선택합니다.
- ▶ 응답 형식(**HTML, 텍스트, HTML 및 텍스트**)을 선택합니다.
- ▶ **확인**을 클릭합니다.
 - ↳ 파일이 압축된 형식으로 Avira 맬웨어 연구 센터 웹 서버에 업로드됩니다.

참고

다음의 경우에는 Avira 맬웨어 연구 센터에 분석 의뢰를 권장합니다.

추론 적중(의심스러운 파일): 검사 중에 Avira 제품에 의해 파일이 의심스러운 파일로 분류되어 격리 저장소로 이동되는 경우: 바이러스 검색 대화 상자나 검사에서 생성된 보고서 파일에 Avira 맬웨어 연구 센터에 의한 파일 분석이 권장된 경우.

의심스러운 파일: 사용자가 의심스러운 파일로 간주하고 이를 격리 저장소로 이동했으나 파일의 바이러스 및 맬웨어 검사 결과가 음성인 경우.

오진 의심: 바이러스 검색이 오진으로 의심되는 경우: Avira 제품이 파일에서 발견 항목을 보고하지만 이 파일이 맬웨어에 감염되었을 가능성이 매우 낮은 경우.


참고

업로드하는 파일의 크기는 압축하지 않은 경우 **20MB**, 압축한 경우 **8MB**로 제한됩니다.

참고

한 번에 하나의 파일만 업로드할 수 있습니다.


격리된 개체를 격리 저장소에서 다른 디렉터리로 복사하려는 경우

- ▶ 격리된 개체를 강조 표시하고  을 클릭합니다.
 - ↳ 디렉터를 선택할 수 있는 **폴더 찾아보기** 대화 상자가 열립니다.
- ▶ 격리된 개체의 복사본을 저장할 디렉터를 선택하고 선택 항목을 확인합니다.
 - ↳ 선택한 격리된 개체가 선택한 디렉터리에 저장됩니다.

참고

격리된 개체는 복원된 파일과 다릅니다. 격리된 개체는 암호화되며 원본 형식으로 실행하거나 읽을 수 없습니다.

격리된 개체의 속성을 텍스트 파일로 내보내려는 경우



- ▶ 격리된 개체를 강조 표시하고  을 클릭합니다.
 - ↳ 선택한 격리된 개체의 데이터가 들어 있는 **격리 - 메모장** 텍스트 파일이 열립니다.
- ▶ 텍스트 파일을 저장합니다.

격리 저장소에서 파일을 복원할 수도 있습니다(장: [격리 저장소: 격리 저장소의 파일 복원 참조](#)).

4.3.12 격리 저장소의 파일 복원



복원 절차를 제어하는 아이콘은 운영 체제에 따라 다릅니다.

- Windows XP:

-  이 아이콘은 파일을 원래의 디렉터리로 복원합니다.
-  이 아이콘은 파일을 사용자가 선택한 디렉터리로 복원합니다.

- Windows Vista:

Microsoft Windows Vista의 경우 현재로서는 제어 센터의 권한이 제한적입니다(예: 디렉터리 및 파일에 대한 액세스). 특정 작업 및 파일 액세스는 확장된 관리자 권한으로 제어 센터에서만 수행할 수 있습니다. 이 확장된 관리자 권한은 검사를 시작할 때마다 검사 프로필을 통해 부여해야 합니다.

-  이 아이콘은 파일을 사용자가 선택한 디렉터리로 복원합니다.
-  이 아이콘은 파일을 원래의 디렉터리로 복원합니다. 이 디렉터리에 액세스하는 데 확장된 관리자 권한이 필요한 경우 이를 요청하는 메시지가 나타납니다.


격리 저장소의 파일을 복원하려면:

경고

이 경우 컴퓨터의 데이터가 손실되고 운영 체제가 손상될 수 있습니다! 예외적인 경우에만 **선택한 개체 복원** 기능을 사용하십시오. 새 검사로 복구할 수 있는 파일만 복원하십시오.

- ✓ 파일을 다시 검사하고 복구합니다.
- ▶ 제어 센터에서 **관리 > 격리 저장소** 섹션을 선택합니다.

참고


전자 메일 및 전자 메일 첨부 파일은 파일 확장명이 ***.eml**인 경우  옵션을 사용하여 복원할 수 있습니다.

파일을 원래의 위치로 복원하려면:

- ▶ 파일을 강조 표시하고 아이콘(Windows XP:  , Windows Vista )을 클릭합니다.


전자 메일에는 이 옵션을 사용할 수 없습니다.

참고

전자 메일 및 전자 메일 첨부 파일은 파일 확장명이 ***.eml**인 경우  옵션을 사용하여 복원할 수 있습니다.


- ↳ 파일을 복원할 것인지 묻는 메시지가 나타납니다.
- ▶ 예를 클릭합니다.
- ↳ 파일이 격리 저장소로 이동하기 전에 있던 디렉터리로 복원됩니다.

지정한 위치로 파일을 복원하려면:

- ▶ 파일을 강조 표시하고  을 클릭합니다.
- ↳ 파일을 복원할 것인지 묻는 메시지가 나타납니다.
- ▶ 예를 클릭합니다.
- ↳ 디렉터를 선택하기 위한 **Windows** 기본 창인 *다른 이름으로 저장*이 나타납니다.
- ▶ 파일을 복원할 디렉터를 선택하고 확인합니다.
- ↳ 선택한 디렉터리로 파일이 복원됩니다.

4.3.13 의심스러운 파일을 격리 저장소로 이동

의심스러운 파일을 격리 저장소로 직접 이동하려면:

- ▶ 제어 센터에서 *관리* > **격리 저장소** 섹션을 선택합니다.
- ▶  을 클릭합니다.
- ↳ **Windows**의 파일 선택 기본 창이 나타납니다.
- ▶ 파일을 선택하고 **열기**를 클릭합니다.
- ↳ 파일이 격리 저장소로 이동합니다.

Avira Scanner를 사용하여 격리 저장소의 파일을 확인할 수 있습니다([격리 저장소: 격리된 파일\(*.qua\) 처리장 참조](#)).

4.3.14 검사 프로필의 파일 형식 수정 또는 삭제

검사 프로필에서 검사할 파일 형식을 추가로 지정하거나 특정 파일 형식을 검사 대상에서 제외하려면(수동 선택 및 사용자 지정 검사 프로필에 대해서만 가능):

- ✓ 제어 센터에서 *PC 보호* > **Scanner** 섹션으로 이동합니다.
- ▶ 편집할 검사 프로필을 마우스 오른쪽 버튼으로 클릭합니다.
- ↳ 그러면 상황에 맞는 메뉴가 나타납니다.
- ▶ **파일 필터**를 선택합니다.
- ▶ 상황에 맞는 메뉴의 오른쪽에 있는 작은 삼각형을 클릭하여 더 확장합니다.
- ↳ 기본, 모든 파일 검사 및 사용자 정의 항목이 나타납니다.

- ▶ 사용자 정의를 선택합니다.
 - ↳ 파일 확장명 대화 상자가 나타나면서 검사 프로파일로 검사할 모든 파일 형식의 목록이 표시됩니다.

검사에서 파일 형식을 제외하려는 경우:

- ▶ 파일 형식을 강조 표시하고 삭제 버튼을 클릭합니다.

검사에 파일 형식을 추가하려는 경우:


- ▶ 파일 형식을 강조 표시합니다.
- ▶ 삽입을 클릭하고 파일 형식의 확장명을 입력란에 입력합니다.

최대 10자까지 입력 가능하며, 앞에 점을 입력하지 않습니다. 와일드카드(* 및 ?)를 사용할 수 있습니다.

4.3.15 검사 프로파일의 바탕 화면 바로 가기 만들기

검사 프로파일에 대한 바탕 화면 바로 가기를 이용하면 Avira 제품 제어 센터에 액세스하지 않고 바탕 화면에서 곧바로 시스템 검사를 시작할 수 있습니다.

검사 프로파일에 대한 바탕 화면 바로 가기를 만들려면

- ✓ 제어 센터에서 *PC 보호* > **Scanner** 섹션으로 이동합니다.
- ▶ 바로 가기를 만들 검사 프로파일을 선택합니다.
- ▶  아이콘을 클릭합니다.
 - ↳ 바탕 화면 바로 가기가 만들어집니다.

4.3.16 이벤트 필터링

Avira 제품의 프로그램 구성 요소에 의해 생성된 이벤트는 제어 센터에서 *관리* > **이벤트**(Windows 운영 체제의 이벤트 표시에 해당)에 표시됩니다. 프로그램 구성 요소는 다음과 같습니다(알파벳 순서).

- Backup
- FireWall
- 도우미 서비스
- Mail Protection
- Real-Time Protection
- Safe Browsing
- 스케줄러
- Scanner

- 업데이트 프로그램
- Web Protection

다음 이벤트 유형이 표시됩니다.



- 정보
- 경고
- 오류
- 검색

표시된 이벤트를 필터링하려면:

- ▶ 제어 센터에서 *관리* > **이벤트** 섹션을 선택합니다.
- ▶ 활성화된 프로그램 구성 요소의 이벤트를 표시하려면 해당 구성 요소의 체크박스를 선택합니다.
 - 또는 -
 - 비활성화된 구성 요소의 이벤트를 숨기려면 프로그램 구성 요소의 체크박스를 선택 취소합니다.
- ▶ 이벤트를 표시하려면 해당 이벤트 유형 체크박스를 선택합니다.
 - 또는 -
 - 이벤트를 숨기려면 해당 이벤트 유형 체크박스를 선택 취소합니다.

4.3.17 검사에서 전자 메일 주소 제외

Mail Protection 검사(허용 목록)에서 제외할 전자 메일 주소(보낸 사람)를 정의하려면:

- ▶ 제어 센터에서 *인터넷 보호* > **Mail Protection**을 선택합니다.
 - ↳ 받는 전자 메일의 목록이 표시됩니다.
- ▶ **Mail Protection** 검사에서 제외할 전자 메일을 강조 표시합니다.
- ▶ 적절한 아이콘을 클릭하여 **Mail Protection** 검사에서 전자 메일을 제외합니다.
 -  선택한 전자 메일 주소에 대해서는 더 이상 바이러스 및 사용자 동의 없이 설치된 프로그램 여부를 검사하지 않습니다.
 -  선택한 전자 메일 주소에 대해 더 이상 스팸 여부를 검사하지 않습니다.
 - ↳ 전자 메일 보낸 사람 주소를 제외 목록에 포함하여 더 이상 바이러스, 맬웨어 또는 스팸을 검사하지 않습니다.

경고

보낸 사람을 완전히 신뢰할 수 있는 경우에만 **Mail Protection** 검사에서 전자 메일 주소를 제외하십시오.



참고

구성의 **Mail Protection > 일반 > 예외** 아래에서 다른 전자 메일을 제외 목록에 추가하거나 전자 메일 주소를 제외 목록에서 제거할 수 있습니다.

4.3.18 스팸 방지 모듈 학습

스팸 방지 모듈에는 학습 데이터베이스가 포함되어 있습니다. 이 학습 데이터베이스에는 사용자별 범주 분류 조건이 기록됩니다. 시간이 지나면서 스팸에 대한 내부 필터, 알고리즘 및 평가 조건이 각 개인의 조건에 맞게 조정됩니다.

학습 데이터베이스를 위해 전자 메일을 범주로 분류하려면:

- ▶ 제어 센터에서 **인터넷 보호 > Mail Protection**을 선택합니다.
 - ↳ 받는 전자 메일의 목록이 표시됩니다.
- ▶ 분류할 전자 메일을 강조 표시합니다.
- ▶ 적절한 아이콘을 클릭하여 전자 메일을 스팸  또는 '정상'  등으로 분류합니다.
 - ↳ 학습 데이터베이스에 전자 메일이 입력되고 다음 스팸 인식 프로세스에 적용됩니다.

참고

Mail Protection > 일반 > 스팸 방지 아래의 구성에서 학습 데이터베이스를 삭제할 수 있습니다.

참고

스팸 방지 모듈은 **IMAP**를 통해 수신된 전자 메일에 대해서는 작동하지 않습니다. 이 때문에 **IMAP**를 통해 받은 전자 메일에는 학습 기능(**정상 전자 메일 - 교육용, 스팸 - 교육용**)을 적용할 수 없습니다. **IMAP** 유형의 전자 메일을 선택한 경우에는 학습 기능이 자동으로 비활성화됩니다.

4.3.19 FireWall의 보안 수준 선택

다양한 보안 수준 중에 선택할 수 있습니다. 선택 항목에 따라 다른 어댑터 규칙 구성 옵션이 제공됩니다.

다음 보안 수준을 사용할 수 있습니다.

낮음

플로딩 및 포트 검사를 검색합니다.

보통

의심스러운 TCP 및 UDP 패키지를 무시합니다.

플로딩 및 포트 검사를 차단합니다.

(기본 수준으로 설정)

높음

네트워크에 컴퓨터를 표시하지 않습니다.

외부로부터의 새 연결을 허용하지 않습니다.

플로딩 및 포트 검사를 차단합니다.

사용자 지정

사용자 정의 규칙: 이 보안 수준을 선택하면 프로그램에서 어댑터 규칙이 수정되었음을 자동으로 인식합니다.

모두 차단

기존의 모든 네트워크 연결을 닫습니다.

참고

Avira FireWall의 미리 정의된 모든 규칙에 대한 기본 보안 수준 설정은 보통입니다.

FireWall의 보안 수준을 선택하려면:

- ▶ 제어 센터에서 *인터넷 보호* > **FireWall** 섹션을 선택합니다.
- ▶ 슬라이더를 필요한 보안 수준으로 이동합니다.
 - ↳ 선택한 보안 수준이 즉시 적용됩니다.

4.3.20 수동으로 백업 만들기

제어 센터의 백업 도구를 사용하면 신속하고 손쉽게 개인 데이터를 백업할 수 있습니다. Avira Backup에서는 미리 백업을 만들 수 있으며 최소한의 리소스로 최근 데이터를 저장하고 보관할 수 있습니다. Avira Backup을 통해 백업 중 데이터의 바이러스 및 맬웨어를 검사할 수 있습니다. 감염된 파일은 저장되지 않습니다.

참고


미러 백업은 버전 백업과 달리 개별 백업 버전을 저장하지 않습니다. 미러 백업은 마지막 백업 시점의 데이터로 구성됩니다. 그러나 저장된 데이터의 파일이 삭제될 경우 다음 백업에서 어떤 일치 작업도 수행되지 않습니다. 즉 삭제된 파일을 백업에서 계속 사용할 수 있습니다.

참고

Avira Backup의 기본 설정에서는 수정된 파일만 저장되며 파일에 대해 바이러스 및 맬웨어를 검사합니다. [Backup > 설정](#)의 구성에서 이러한 설정을 변경할 수 있습니다.

백업 도구를 사용하여 데이터를 저장하려면:

- ▶ 제어 센터에서 *PC 보호 > Backup* 섹션을 선택합니다.
 - ↳ 미리 설정된 백업 프로필이 나타납니다.
- ▶ 미리 설정된 백업 프로필 중 하나를 선택합니다.
 - 또는-
 - 백업 프로필 **수동 선택**을 변경합니다.
 - 또는-
 - 새 백업 프로필을 만듭니다.
- ▶ 선택한 프로필의 저장 위치를 **대상 디렉터리** 상자에 입력합니다.

백업의 저장 위치는 해당 컴퓨터, 연결된 네트워크 드라이브 또는 이동식 디스크(예: USB 스틱 또는 디스켓)의 디렉터리가 될 수 있습니다.
- ▶  아이콘을 클릭합니다.
 - ↳ **Avira Backup** 창이 나타나며 백업이 시작합니다. 백업의 상태 및 결과가 백업 창에 표시됩니다.



백업 프로필을 수정하려는 경우:

- ▶ 검사 프로필에서 **수동 선택** 파일 트리를 확장하여 저장할 모든 드라이브 및 디렉터리를 엽니다.
 - + 아이콘 클릭: 다음 디렉터리 수준이 표시됩니다.
 - - 아이콘 클릭: 다음 디렉터리 수준이 숨겨집니다.
- ▶ 각 디렉터리 수준의 상자를 클릭하여 저장할 노드 및 디렉터리를 강조 표시합니다.

디렉터리를 선택할 때 다음 옵션을 사용할 수 있습니다.


- ▶ 하위 디렉터리를 포함한 디렉터리(검정색 확인 표시)
- ▶ 한 디렉터리의 하위 디렉터리만 선택(회색 확인 표시, 하위 디렉터리는 검정색 확인 표시)
- ▶ 디렉터리 선택 안 함(확인 표시 없음)

새 백업 프로필을 만들려는 경우:

- ▶  새 프로필 만들기 아이콘을 클릭합니다.
 - ↳ 이전에 만든 프로필 아래에 새 프로필이 나타납니다.
- ▶ 적절한 경우  아이콘을 클릭하여 백업 프로필의 이름을 지정합니다.
- ▶ 각 디렉터리 수준의 상자를 클릭하여 저장할 노드 및 디렉터리를 강조 표시합니다.
 - ▶ 디렉터리를 선택할 때 다음 옵션을 사용할 수 있습니다.
 - 하위 디렉터리를 포함한 디렉터리(검정색 확인 표시)
 - 한 디렉터리의 하위 디렉터리만 선택(회색 확인 표시, 하위 디렉터리는 검정색 확인 표시)
 - 디렉터리 선택 안 함(확인 표시 없음)

4.3.21 자동 데이터 백업 만들기

여기서는 자동 데이터 백업을 만들기 위해 작업을 시작하는 방법을 소개합니다.

- ▶ 제어 센터에서 *관리* > *스케줄러* 섹션을 선택합니다.
- ▶  아이콘을 클릭합니다.
 - ↳ 작업의 이름 및 설명 대화 상자가 나타납니다.
- ▶ 작업 이름과 적절한 경우 설명을 입력합니다.
- ▶ 다음을 클릭합니다.
 - ↳ 작업 유형 대화 상자가 나타납니다.
- ▶ **Backup** 작업을 선택합니다.
- ▶ 다음을 클릭합니다.
 - ↳ 프로필 선택 대화 상자가 나타납니다.
- ▶ 검사할 프로필을 선택합니다.

참고

저장 위치가 지정된 백업 프로파일만 표시됩니다.


- ▶ 다음을 클릭합니다.
 - ↳ 작업 시간 대화 상자가 나타납니다.
- ▶ 검사 시간을 선택합니다.
 - 즉시
 - 매일
 - 매주
 - 간격
 - 단일
 - 로그인
 - 플러그 앤 플레이
 - 백업 프로파일의 저장 위치로 선택된 이동식 디스크가 컴퓨터에 연결된 경우 항상 플러그 앤 플레이 이벤트에 대해 백업이 만들어집니다. 백업 이벤트 플러그 앤 플레이를 사용하려면 **USB** 스틱을 저장 위치로 입력해야 합니다.
- ▶ 선택 항목에 따라 날짜를 지정합니다.
- ▶ 다음 추가 옵션을 선택합니다. 선택 가능 여부는 작업 유형에 따라 다릅니다.


시간이 만료된 경우 작업 반복


컴퓨터 전원이 꺼지는 등의 이유로 인해 필요할 때 수행할 수 없었던 지난 작업을 수행합니다.


- ▶ 다음을 클릭합니다.
 - ↳ 디스플레이 모드 선택 대화 상자가 나타납니다.
- ▶ 작업 창의 디스플레이 모드를 선택합니다.
 - 최소화: 진행률 표시줄만
 - 최대화: 전체 백업 창
 - 표시하지 않음: 백업 창 표시하지 않음
- ▶ 마침을 클릭합니다.
 - ↳ 새로 만든 작업이 상태가 활성화되어(체크 표시) **관리 > 스케줄러** 섹션의 시작 페이지에 나타납니다.
- ▶ 필요한 경우 수행하지 않을 작업은 비활성화합니다.


작업을 더 자세히 정의하려면 다음 아이콘을 사용합니다.

 작업의 속성 보기

 작업 편집

 작업 삭제

 작업 시작

 작업 중지

5. Scanner

Scanner 구성 요소를 사용하면 바이러스 및 사용자 동의 없이 설치된 프로그램에 대해 대상 지정 검사(수동 검사)를 실시할 수 있습니다. 감염된 파일을 검사할 때 다음 옵션을 사용할 수 있습니다.

- **상황에 맞는 메뉴를 통한 시스템 검사**
 상황에 맞는 메뉴(마우스 오른쪽 버튼 클릭 - **Avira를 사용하여 선택한 파일 검사**)를 통한 시스템 검사는 개별 파일이나 디렉터리를 검사할 때 권장합니다. 상황에 맞는 메뉴를 통해 시스템을 검사할 때 제어 센터를 먼저 시작할 필요가 없다는 장점도 있습니다.
- **끌어서 놓기를 사용한 시스템 검사**
 파일 또는 디렉터리를 제어 센터의 프로그램 창으로 끌면 **Scanner**가 해당 파일 또는 디렉터리와 모든 하위 디렉터를 검사합니다. 예를 들어, 데스크톱에 저장한 개별 파일 및 디렉터를 검사하려는 경우 이 절차를 이용하는 것이 좋습니다.
- **프로필을 사용한 시스템 검사**
 특정 디렉터리 및 드라이브(예: 정기적으로 새 파일을 저장하는 작업 디렉터리 또는 드라이브)를 정기적으로 검사하려는 경우 이 절차를 이용하는 것이 좋습니다. 그러면 새로 검사할 때마다 디렉터리 및 드라이브를 선택할 필요 없이 해당 프로필을 사용하여 선택하면 됩니다.
- **스케줄러를 통한 시스템 검사**
 스케줄러를 사용하여 원하는 시간에 검사를 수행할 수 있습니다

Rootkits 또는 부트 섹터 바이러스를 검사하거나 활성 프로세스를 대상으로 검사할 때 특별한 프로세스가 필요합니다. 다음 옵션을 사용할 수 있습니다.

- 검사 프로필 **Rootkits 및 활성 맬웨어** 검사를 통해 **rootkits** 검사
- 검사 프로필 **활성 프로세스**를 통해 활성 프로세스 검사
- 기타 메뉴의 **부트 레코드 검사** 메뉴 명령을 통해 부트 섹터 바이러스 검사

6. 업데이트

바이러스 백신 소프트웨어의 효과는 해당 프로그램, 특히 바이러스 정의 파일 및 검사 엔진이 얼마나 최신 버전인가에 따라 다릅니다. 통상적인 업데이트를 수행할 수 있도록 업데이트 프로그램 구성 요소가 Avira 제품에 통합되었습니다. 업데이트 프로그램을 통해 Avira 제품은 항상 최신 상태를 유지하고 매일 나타나는 새로운 바이러스를 처리할 수 있습니다. 업데이트 프로그램에서는 다음 구성 요소를 업데이트합니다.

- 바이러스 정의 파일:
 바이러스 정의 파일에는 유해한 프로그램의 바이러스 패턴이 있으며, Avira 제품은 이 패턴을 사용하여 바이러스 및 맬웨어를 검사하고 감염된 개체를 복구합니다.
- 검사 엔진:
 검사 엔진에는 Avira 제품이 바이러스 및 맬웨어를 검사하는 데 사용하는 방법이 들어 있습니다.
- 프로그램 파일(제품 업데이트):
 제품 업데이트용 업데이트 패키지에서는 개별 프로그램 구성 요소에서 사용 가능한 추가 기능을 제공합니다.

업데이트는 바이러스 정의 파일, 검사 엔진 및 제품이 최신 버전인지 확인하고 필요하다면 업데이트를 구현합니다. 제품 업데이트 후에는 컴퓨터 시스템을 다시 시작해야 할 수도 있습니다. 바이러스 정의 파일 및 검사 엔진만 업데이트된 경우에는 컴퓨터를 다시 시작할 필요가 없습니다.

제품 업데이트시 재부팅이 필요하다면 업데이트 계속 또는 추후 업데이트 관련 알림 수신 중 하나를 선택할 수 있습니다. 업데이트를 계속하는 경우 재부팅 시점을 선택할 수 있습니다.

추후 업데이트 관련 알림 수신을 선택한 경우에도 바이러스 정의 파일, 검사 엔진은 업데이트가 진행됩니다. 단 제품은 업데이트 되지 않습니다.

참고

재부팅하지 않으면 업데이트가 완료되지 않습니다.

참고

보안을 유지하기 위해 업데이트 프로그램에서는 컴퓨터의 Windows 호스트 파일이 변경되었는지, 이를테면 업데이트 URL이 맬웨어에 의해 수정되어 업데이트 프로그램이 원치 않는 다운로드 사이트로 전환되는지 여부를 검사합니다. Windows 호스트 파일이 수정된 경우 이는 업데이트 프로그램 보고서 파일에 표시됩니다.

업데이트는 2시간 간격으로 자동 수행됩니다.

제어 센터의 스케줄러에서는 지정된 간격대로 업데이트 프로그램에서 수행할 추가 업데이트 작업을 만들 수 있습니다. 또한 다음 위치에 업데이트를 수동으로 시작하는 옵션도 있습니다.

- 제어 센터: **업데이트** 메뉴와 **상태** 섹션
- 트레이 아이콘의 상황에 맞는 메뉴에서

인터넷에서 제조업체의 웹 서버를 통해 업데이트를 얻을 수 있습니다. 기존 네트워크 연결이 Avira의 다운로드 서버와의 기본 연결 방식입니다. ([구성 > 업데이트](#))에서 이 설정을 바꿀 수 있습니다.

7. FireWall

Avira Internet Security에서는 컴퓨터 설정에 따라 수신 및 발신 데이터 트래픽을 관리할 수 있습니다.

- Avira FireWall

Windows 7 이하 운영 체제인 경우 Avira Internet Security에는 Avira FireWall이 포함됩니다.

8. Backup

데이터 백업본을 만들 때 다양한 옵션을 사용할 수 있습니다.

백업 도구를 통한 백업

백업 도구를 사용하여 백업 프로필을 선택하거나 만들 수 있으며 선택한 프로필의 백업을 수동으로 시작할 수 있습니다.

스케줄러의 백업 작업을 통한 백업

스케줄러를 사용하면 예약된 백업 작업이나 이벤트 제어 백업 작업을 만들 수 있습니다. 스케줄러는 백업 작업을 자동으로 실행합니다. 이 프로세스는 특정 데이터를 정기적으로 백업하려는 경우에 특히 유용합니다.

9. FAQ, 팁

이 장에서는 Avira 제품의 문제 해결 및 팁에 대해 안내합니다.

- 참조:문제 발생 시 도움말
- 참조:바로 가기
- 참조: Windows 보안 센터(Windows XP 및 Vista) 또는 Windows 관리 센터(Windows 7 및 8) 장

9.1 문제 발생 시 도움말

여기에는 가능한 문제 원인 및 해결 방법에 대한 정보가 제공됩니다.

- 라이선스 파일을 열 수 없습니다.라는 오류 메시지가 표시됩니다.
- 업데이트하려고 할 때 파일을 다운로드하는 중 연결에 실패했습니다.라는 오류 메시지가 표시됩니다.
- 바이러스 및 맬웨어를 이동하거나 삭제할 수 없습니다.
- 트레이 아이콘의 상태가 비활성화되었습니다.
- 데이터 백업을 수행하면 컴퓨터 속도가 너무 느립니다.
- Firewall이 활성화되는 즉시 Avira Real-Time Protection 및 Avira Mail Protection에 보고합니다.
- Avira Mail Protection이 작동하지 않습니다.
- Avira Firewall이 호스트 컴퓨터에 설치되고 Avira Firewall의 보안 수준이 보통 또는 높음으로 설정된 경우에는 가상 컴퓨터(예: VMWare, Virtual PC 등)에서 네트워크에 연결할 수 없습니다.
- Avira Firewall의 보안 수준이 보통 또는 높음으로 설정된 경우 VPN(가상 사설망) 연결이 차단됩니다.
- TLS 연결을 통해 보낸 전자 메일이 Mail Protection에 의해 차단되었습니다.
- Webchat이 작동하지 않습니다. 채팅 메시지가 표시되지 않습니다.

라이선스 파일을 열 수 없습니다.라는 오류 메시지가 표시됩니다.

이유: 이 파일은 암호화되어 있습니다.

- ▶ 라이선스를 활성화하려는 경우 라이선스 파일을 열 필요 없이 프로그램 디렉터리에 저장하기만 하면 됩니다.

업데이트하려고 할 때 *파일을 다운로드하는 중 연결에 실패했습니다.*라는 오류 메시지가 표시됩니다.

이유: 인터넷 연결이 비활성 상태입니다. 인터넷 연결이 설정되지 않았습니다.

- ▶ WWW 또는 전자 메일과 같은 다른 인터넷 서비스가 작동하는지 테스트합니다. 작동하지 않을 경우 인터넷 연결을 설정하십시오.

이유: 프록시 서버에 연결할 수 없습니다.

- ▶ 프록시 서버에 대한 로그인이 변경되었는지 확인하고 필요한 경우 구성에 적용합니다.

이유: 사용자의 개인 Firewall에서 *update.exe* 파일을 완전히 승인하지 않았습니다.

- ▶ 사용자의 개인 Firewall에서 *update.exe* 파일을 완전히 승인했는지 확인합니다.

그렇지 않은 경우 다음을 수행합니다.

- ▶ 구성(고급 모드)의 **PC 보호 > 업데이트**에서 설정을 확인합니다.

바이러스 및 맬웨어를 이동하거나 삭제할 수 없습니다.

이유: 파일이 Windows를 통해 로드되어 활성 상태입니다.

- ▶ Avira 제품을 업데이트합니다.
- ▶ 운영 체제 Windows XP를 사용하는 경우 시스템 복원을 비활성화합니다.
- ▶ 안전 모드로 컴퓨터를 시작합니다.
- ▶ Avira 제품의 구성(고급 모드)을 시작합니다.
- ▶ **Scanner > 검사 > 파일 > 모든 파일**을 선택하고 창에서 **확인**을 클릭합니다.
- ▶ 모든 로컬 드라이브에 대한 검사를 시작합니다.
- ▶ 표준 모드로 컴퓨터를 시작합니다.
- ▶ 표준 모드에서 검사를 수행합니다.
- ▶ 다른 바이러스나 맬웨어가 발견되지 않으면 가능한 한 시스템 복원을 활성화하고 사용합니다.

트레이 아이콘의 상태가 비활성화되었습니다.

이유: Avira Real-Time Protection이 사용하지 않도록 설정되었습니다.

- ▶ 제어 센터에서 **상태**를 클릭하고 **PC 보호** 영역에서 *Real-Time Protection*을 사용하도록 설정합니다.

-또는-

- ▶ 마우스 오른쪽 버튼으로 트레이 아이콘을 클릭하여 상황에 맞는 메뉴를 엽니다. **Real-Time Protection** 사용을 클릭합니다.

이유: Avira Real-Time Protection이 Firewall에 의해 차단되었습니다.

- ▶ Firewall 구성에서 AntiVir Guard에 대한 일반 승인을 정의합니다. Avira Real-Time Protection은 주소 127.0.0.1(localhost)로만 작동합니다. 인터넷 연결이 설정되지 않습니다. Avira Mail Protection도 이와 동일하게 작동합니다.

그렇지 않은 경우 다음을 수행합니다.

- ▶ Avira Real-Time Protection 서비스 시작 유형을 확인합니다. 필요할 경우 작업 표시줄에서 **시작 > 설정 > 제어판**을 선택하여 서비스를 사용하도록 설정합니다. 더블클릭하여 구성 패널 **서비스**를 시작합니다(Windows 2000 및 Windows XP에서 서비스 애플릿은 하위 디렉터리 **관리 도구**에 있음). **Avira Real-Time Protection** 항목을 찾습니다. 시작 유형이 자동이어야 하고 상태가 시작이어야 합니다. 필요한 경우 관련 줄을 선택하고 **시작** 버튼을 클릭하여 서비스를 수동으로 시작합니다. 오류 메시지가 표시되면 이벤트 표시를 확인합니다.

데이터 백업을 수행하면 컴퓨터 속도가 너무 느립니다.

이유: 백업 절차 중에는 Avira Real-Time Protection에서 백업 절차에 사용되고 있는 모든 파일을 검사합니다.

- ▶ 구성에서 **Real-Time Protection > 검사 > 예외**를 선택하고 백업 소프트웨어의 프로세스 이름을 입력합니다.

활성화한 직후에 **Firewall**에서 **Avira Real-Time Protection**과 **Avira Mail Protection**을 보고합니다.

이유: Avira Real-Time Protection 및 Avira Mail Protection와의 통신은 TCP/IP 인터넷 프로토콜을 통해 이루어집니다. Firewall은 이 프로토콜을 통해 모든 연결을 모니터링합니다.

- ▶ Avira Real-Time Protection 및 Avira Mail Protection에 대한 일반 승인을 정의합니다. Avira Real-Time Protection은 주소 127.0.0.1(localhost)로만 작동합니다. 인터넷 연결이 설정되지 않습니다. Avira Mail Protection도 이와 동일하게 작동합니다.

Avira Mail Protection이 작동하지 않습니다.

Avira Mail Protection과 관련하여 문제가 발생하는 경우 다음 검사 목록을 사용하여 Avira Mail Protection이 올바르게 작동하는지 확인합니다.

검사 목록

- ▶ 메일 클라이언트가 Kerberos, APOP 또는 RPA를 통해 서버에 로그인했는지 확인합니다. 이러한 확인 방법은 현재 지원되지 않습니다.
- ▶ 메일 클라이언트가 SSL(TLS - Transport Layer Security이라고도 함)을 통해 서버에 보고하는지 확인합니다. Avira Mail Protection에서는 SSL을 지원하지 않으므로 암호화된 SSL 연결을 종료합니다. Mail Protection으로 보호되지 않은 상태에서 암호화된 SSL 연결을 사용하려면 Mail Protection에서 연결을 모니터링하지 않는 포트를 사용해야 합니다. 구성의 **Mail Protection > 검사**에서 Mail Protection을 통해 모니터링된 포트를 구성할 수 있습니다.
- ▶ Avira Mail Protection 서비스가 활성화되었습니까? 필요할 경우 작업 표시줄에서 **시작 > 설정 > 제어판**을 선택하여 서비스를 사용하도록 설정합니다. 더블클릭하여 구성 패널 서비스를 시작합니다(Windows 2000 및 Windows XP에서 서비스 애플릿은 하위 디렉터리 *관리 도구*에 있음). Avira Mail Protection 항목을 찾습니다. 시작 유형이 자동이어야 하고 상태가 시작이어야 합니다. 필요한 경우 관련 줄을 선택하고 **시작** 버튼을 클릭하여 서비스를 수동으로 시작합니다. 오류 메시지가 표시되면 이벤트 표시를 확인합니다. 이 작업이 성공적으로 수행되지 않으면 **시작 > 설정 > 제어판 > 프로그램 추가/제거**를 통해 Avira 제품을 완전히 제거했다가 컴퓨터를 다시 시작한 후 Avira 프로그램을 다시 설치해야 합니다.

일반

TLS(전송 계층 보안)라고도 하는 SSL(Secure Sockets Layer)을 통해 암호화된 POP3 연결은 현재 보호할 수 없으며 무시됩니다.

메일 서버에 대한 확인은 현재 암호를 통해서만 지원됩니다. Kerberos 및 RPA는 현재 지원되지 않습니다.

Avira 제품은 보내는 전자 메일에서 바이러스 및 사용자 동의 없이 설치된 프로그램에 대해 검사하지 않습니다.

참고

보안에 허점이 생기지 않도록 Microsoft 업데이트를 정기적으로 설치하는 것이 좋습니다.

Avira Firewall이 호스트 컴퓨터에 설치되고 **Avira Firewall**의 보안 수준이 *보통* 또는 *높음*으로 설정된 경우에는 가상 컴퓨터(예: **VMWare, Virtual PC** 등)에서 네트워크에 연결할 수 없습니다.

Avira Firewall이 가상 컴퓨터(예: VMWare, Virtual PC 등)가 실행 중인 컴퓨터에 설치되고 Avira Firewall의 보안 수준이 *보통* 또는 *높음*으로 설정된 경우에는 가상 컴퓨터에 대한 모든

네트워크 연결이 **Firewall**에 의해 차단됩니다. 보안 수준이 **낮음**으로 설정되어 있으면 **FireWall**에서 네트워크 연결을 허용합니다.

이유: 가상 시스템은 소프트웨어를 통해 네트워크 카드를 에뮬레이션합니다. 이 에뮬레이션은 게스트 시스템의 데이터 패키지를 특수한 패키지(**UDP** 패키지)로 캡슐화하고 외부 게이트웨이를 통해 호스트 시스템에 라우팅합니다. **Avira FireWall**은 **보통**의 보안 수준부터 시작하여 외부에서 들어오는 이러한 패키지를 차단합니다.

이러한 동작이 발생하지 않도록 하려면 다음을 수행합니다.

- ▶ 제어 센터로 이동하여 **인터넷 보호 > FireWall** 섹션을 선택합니다.
- ▶ 구성 버튼을 클릭합니다.
구성 대화 상자가 표시됩니다. 구성 섹션 **응용 프로그램 규칙**이 표시됩니다.
- ▶ **고급 모드** 옵션을 활성화합니다.
- ▶ 구성 섹션 **어댑터 규칙**을 선택합니다.
- ▶ **규칙 추가**를 클릭합니다.
- ▶ **들어오는 규칙** 섹션에서 **UDP**를 선택합니다.
- ▶ 규칙 이름 섹션에 규칙 이름을 입력합니다.
- ▶ **확인**을 클릭합니다.
- ▶ 규칙이 **모든 IP 패킷 거부** 규칙 바로 위에 있는지 확인합니다.

경고

이 규칙은 **UDP** 패킷을 필터링하지 않고 허용하므로 위험 가능성이 있습니다. 가상 시스템 작업 후에 이전 보안 수준으로 변경합니다.

Avira Firewall의 보안 수준이 **보통**또는 **높음**으로 설정된 경우 **VPN(가상 사설망)** 연결이 차단됩니다.

이유: 기본적으로 사전 설정된 규칙을 준수하지 않는 모든 패킷을 버립니다. **VPN** 소프트웨어가 보낸 패킷(**GRE** 패킷이라고도 함)은 다른 범주에 맞지 않으므로 이 규칙에 의해 필터링됩니다.

VPN 연결 규칙을 **Avira FireWall** 구성의 **어댑터 규칙**에 추가합니다. 이 규칙은 모든 **VPN** 관련 패킷을 허용합니다.

TLS 연결을 통해 보낸 전자 메일이 **Mail Protection**에 의해 차단되었습니다.

이유: **TLS(Transport Layer Security: 인터넷에서 데이터 전송을 위한 암호화 프로토콜)**는 현재 **Mail Protection**에서 지원하지 않습니다. 전자 메일을 보내는 데 사용할 수 있는 옵션은 다음과 같습니다.

- ▶ 25번 포트는 SMTP에 사용되므로 다른 포트를 사용합니다. 그러면 Mail Protection에서 해당 포트에 대한 모니터링을 생략합니다.
- ▶ TLS 암호화된 연결을 해제하고 전자 메일 클라이언트에서 TLS 지원을 비활성화합니다.
- ▶ 구성의 **Mail Protection > 검사**에서 Mail Protection을 통한 보내는 전자 메일 모니터링을 (일시적으로) 사용하지 않도록 설정합니다.

웹 채팅 작동 불가능: 채팅 메시지가 표시되지 않고 데이터가 브라우저에 로드 중입니다.

이 현상은 'transfer-encoding= chunked'로 설정된 HTTP 프로토콜을 기반으로 한 채팅 중에 발생할 수 있습니다.

이유: Web Protection은 전송된 데이터가 웹 브라우저에 로드되기 전에 해당 데이터에 대해 바이러스 및 사용자 동의 없이 설치된 프로그램을 먼저 검사합니다. Web Protection은 'transfer-encoding= chunked'로 설정된 데이터 전송 시 메시지 길이나 데이터 볼륨을 확인하지 못합니다.

- ▶ 웹 채팅의 URL 구성을 예외로 입력합니다(구성: **Web Protection > 검사 > 예외** 참조).

9.2 바로 가기

키보드 명령 - 바로 가기라고도 하며, 이를 사용하여 프로그램을 빠르게 탐색하고 개별 모듈을 검색하며, 작업을 시작할 수 있습니다.

다음은 사용 가능한 키보드 명령에 대한 개요입니다. 도움말의 해당 장에서 기능에 대한 세부 지침을 찾아 볼 수 있습니다.

9.2.1 대화 상자에서

바로 가기	설명
Ctrl + Tab Ctrl + Page down	제어 센터에서 탐색 다음 섹션으로 이동합니다.
Ctrl + Shift + Tab Ctrl + Page up	제어 센터에서 탐색 이전 섹션으로 이동합니다.

←↑→↓	구성 섹션에서 탐색 먼저 마우스를 사용하여 구성 섹션으로 포커스를 이동합니다. 표시된 드롭다운 목록의 옵션 간에 또는 옵션 그룹의 여러 옵션 간에 변경합니다.
Tab	다음 옵션 또는 옵션 그룹으로 변경합니다.
Shift+Tab	이전 옵션 또는 옵션 그룹으로 변경합니다.
Space	활성 옵션이 체크박스일 경우 체크박스를 활성화하거나 비활성화합니다.
Alt+밑줄 문자	옵션을 선택하거나 명령을 시작합니다.
Alt + ↓ F4	선택한 드롭다운 목록을 엽니다.
Esc	선택한 드롭다운 목록을 닫습니다. 명령을 취소하고 대화 상자를 닫습니다.
Enter	활성 옵션이나 버튼에 대한 명령을 시작합니다.

9.2.2 도움말에서

바로 가기	설명
Alt + Space	시스템 메뉴를 표시합니다.
Alt + Tab	도움말과 열려 있는 다른 창 간에 전환합니다.
Alt + F4	도움말을 닫습니다.
Shift + F10	도움말의 상황에 맞는 메뉴를 표시합니다.

Ctrl + Tab	탐색 창의 다음 섹션으로 이동합니다.
Ctrl + Shift + Tab	탐색 창의 이전 섹션으로 이동합니다.
Page up	목차, 색인 또는 검색 결과 목록에서 위에 표시된 제목으로 변경합니다.
Page down	목차, 색인 또는 검색 결과 목록에서 현재 제목 아래에 표시된 제목으로 변경합니다.
Page up Page down	제목을 검색합니다.

9.2.3 제어 센터에서

일반

바로 가기	설명
F1	도움말 표시
Alt + F4	제어 센터 닫기
F5	새로 고침
F8	구성 열기
F9	업데이트 시작

검사 섹션

바로 가기	설명
F2	선택한 프로필 이름 바꾸기
F3	선택한 프로필을 사용하여 검사 시작

F4	선택한 프로필에 대한 바탕 화면 링크 만들기
Ins	새 프로필 만들기
Del	선택한 프로필 삭제

FireWall 섹션

바로 가기	설명
Return	속성

격리 섹션

바로 가기	설명
F2	개체 다시 검사
F3	개체 복원
F4	개체 보내기
F6	개체를 다음으로 복원...
Return	속성
Ins	파일 추가

Del	개체 삭제
------------	-------

스케줄러 섹션

바로 가기	설명
F2	작업 편집
Return	속성
Ins	새 작업 삽입
Del	작업 삭제

보고서 섹션

바로 가기	설명
F3	보고서 파일 표시
F4	보고서 파일 인쇄
Return	보고서 표시
Del	보고서 삭제

이벤트 섹션

바로 가기	설명
F3	이벤트 내보내기
Return	이벤트 표시

Del	이벤트 삭제
------------	--------

9.3 Windows 보안 센터

- Windows XP 서비스 팩 2 ~ Windows Vista -

9.3.1 일반

Windows 보안 센터에서는 컴퓨터 상태를 확인하여 중요한 보안 측면을 검사합니다.

이러한 중요한 측면 중 하나에서 문제가 발견되면(예: 오래된 바이러스 백신 프로그램), 보안 센터는 알림을 표시하고 컴퓨터 보호를 향상시키는 방법에 대한 권장 사항을 제공합니다.

9.3.2 Windows 보안 센터와 Avira 제품

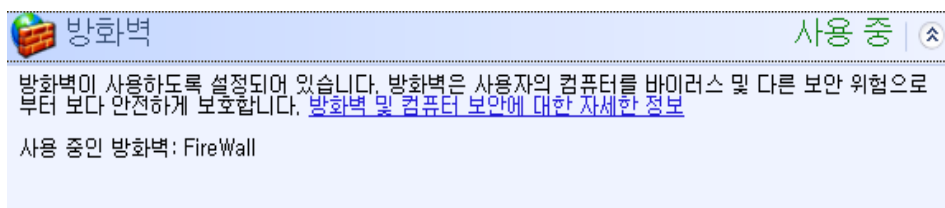
FireWall

보안 센터에서 Firewall에 대한 다음 정보를 받을 수 있습니다.

- [Firewall 활성화/FireWall 켜짐](#)
- [Firewall 비활성화/FireWall 꺼짐](#)

Firewall 활성화/FireWall 켜짐

Avira 제품을 설치하고 나서 Windows 방화벽을 끄면 다음 메시지가 표시됩니다.



Firewall 비활성화/FireWall 꺼짐

Avira FireWall을 비활성화하는 즉시 다음 메시지가 표시됩니다.

방화벽
사용 안 함 |

방화벽이 사용하지 않도록 설정되어 있습니다. 방화벽은 사용자의 컴퓨터에 손상을 줄 수 있는 인터넷 콘텐츠로부터 사용자의 컴퓨터를 안전하게 보호하도록 돕습니다. 이 문제를 해결하는 방법을 보려면 [권장 사항]을 클릭하십시오. [방화벽 및 컴퓨터 보안에 대한 자세한 정보](#)

사용 중지 마닌 방화벽: FireWall

권장 사항(R)...

참고
제어 센터의 상태 탭을 통해 Avira FireWall을 활성화하거나 비활성화할 수 있습니다.

경고
Avira FireWall을 해제하면 권한이 없는 사용자가 네트워크나 인터넷을 통해 컴퓨터에 액세스할 수도 있습니다.

바이러스 방지 소프트웨어/악의적인 소프트웨어로부터 보호

Windows 보안 센터에서 바이러스 방지에 대한 다음 정보를 받을 수 있습니다.

- 바이러스 방지 기능을 찾을 수 없음
- 바이러스 방지 기능이 오래됨
- 바이러스 방지 기능 설정
- 바이러스 방지 기능 해제
- 바이러스 방지 기능이 모니터링되지 않음

바이러스 방지 기능을 찾을 수 없음

Windows 보안 센터에서 사용자의 컴퓨터를 확인하여 바이러스 방지 소프트웨어를 찾을 수 없으면 다음과 같은 Windows 보안 센터 정보가 나타납니다.

바이러스 백신
찾을 수 없음 |

Windows가 이 컴퓨터에서 바이러스 백신 소프트웨어를 찾지 못했습니다. 바이러스 백신 소프트웨어는 사용자의 컴퓨터를 바이러스 및 다른 보안 위협으로부터 보다 안전하게 보호합니다. 사용자가 수행할 수 있는 작업을 보려면 [권장 사항]을 클릭하십시오. [바이러스 백신 소프트웨어 및 컴퓨터 보안에 대한 자세한 정보](#)

참고: Windows에서 모든 바이러스 백신 프로그램을 감지하지는 못합니다.

권장 사항(E)...

참고

바이러스와 사용자 동의 없이 설치된 기타 프로그램으로부터 컴퓨터를 보호하려면 컴퓨터에 Avira 제품을 설치하여 Avira 제품을 설치하십시오.

바이러스 방지 기능이 오래됨

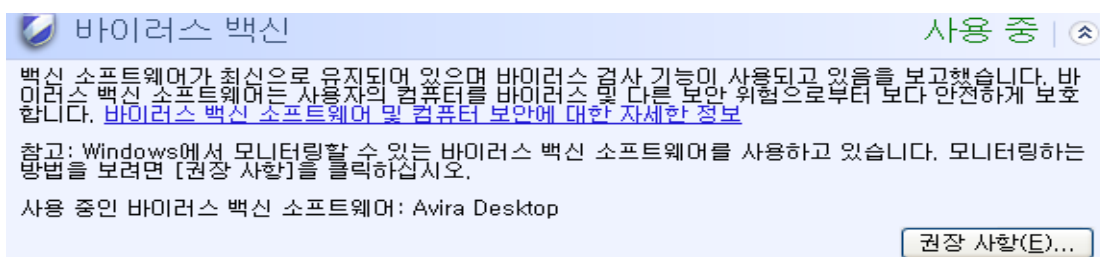
Windows XP 서비스 팩 2 또는 Windows Vista를 설치하고 Avira 제품을 설치하거나 Avira 제품이 이미 설치된 시스템에 Windows XP 서비스 팩 2 또는 Windows Vista를 설치하는 경우 다음 메시지가 표시됩니다.


참고

Windows 보안 센터에서 Avira 제품을 최신 상태로 인식하도록 하려면 업데이트를 수행해야 합니다. 업데이트를 수행하여 시스템을 업데이트합니다.

바이러스 방지 기능 설정

Avira 제품을 설치한 후 후속 업데이트를 수행하고 나면 다음 메시지가 표시됩니다.



Avira 제품이 현재 최신 상태이며 Avira Real-Time Protection을 사용하도록 설정되어 있습니다.

바이러스 방지 기능 해제

Avira Real-Time Protection을 사용하지 않도록 설정하거나 Real-Time Protection 서비스를 중지하면 다음 메시지가 표시됩니다.

바이러스 백신
사용 안 함 |

바이러스 프로그램이 사용되고 있지 않습니다. 바이러스 백신 소프트웨어는 사용자의 컴퓨터를 바이러스 및 다른 보안 위협으로부터 보다 안전하게 보호합니다. 사용자가 수행할 수 있는 작업을 보려면 [권장 사항]을 클릭하십시오. [바이러스 백신 소프트웨어 및 컴퓨터 보안에 대한 자세한 정보](#)

참고: Windows에서 모든 바이러스 백신 프로그램을 검색하지는 못합니다.

검색된 바이러스 백신 프로그램: Avira Desktop

권장 사항(E)...

참고
 제어 센터에서 상태 섹션에서 Avira Real-Time Protection을 사용하거나 사용하지 않도록 설정할 수 있습니다. 작업 표시줄에 빨간색 우산이 펼쳐 있으면 AntiVir Real-Time Protection이 활성화되어 있는 것입니다.

바이러스 방지 기능이 모니터링되지 않음

Windows 보안 센터에서 다음 메시지를 받을 경우 바이러스 방지 소프트웨어를 직접 모니터링하도록 설정한 것입니다.

바이러스 백신
모니터링하지 않음 |

사용자가 직접 관리하는 바이러스 백신 소프트웨어를 사용하고 있다고 선택했습니다. 사용자의 컴퓨터를 바이러스 및 다른 보안 위협으로부터 안전하게 보호하기 위해 바이러스 백신 소프트웨어를 사용하고 최신으로 유지하고 있는지 확인하십시오. [바이러스 백신 소프트웨어 및 컴퓨터 보안에 대한 자세한 정보](#)

권장 사항(E)...

참고
 Windows Vista에서는 이 기능을 지원하지 않습니다.

참고
 Avira 제품에서는 Windows 보안 센터를 지원합니다. **권장 사항** 버튼을 사용하여 언제든지 이 옵션을 활성화할 수 있습니다.

참고
 Windows XP 서비스 팩 2 또는 Windows Vista를 설치한 경우에도 바이러스 방지 솔루션이 필요합니다. Windows는 바이러스 방지 소프트웨어를 모니터링하지만 바이러스 방지 기능 자체가 포함되어 있지는 않습니다. 따라서 추가 바이러스 백신 솔루션 없이는 바이러스 및 기타 맬웨어로부터 보호될 수 없습니다.

9.4 Windows 관리 센터

- Windows 7 및 Windows 8 -

9.4.1 일반

참고:

Windows 7부터 **Windows** 보안 센터가 **Windows** 관리 센터로 이름이 변경되었습니다. 이 섹션에서는 모든 보안 옵션의 상태를 찾아볼 수 있습니다.

Windows 관리 센터에서는 컴퓨터 상태를 확인하여 중요한 보안 측면을 검사합니다. Windows 관리 센터는 작업 표시줄에 있는 작은 깃발 표시를 클릭하여 액세스하거나 **제어판 > 관리 센터**에서 액세스할 수 있습니다.

이러한 중요한 측면 중 하나에서 문제가 발견되면(예: 오래된 바이러스 백신 프로그램), 관리 센터는 알림을 표시하고 컴퓨터 보호를 향상시키는 방법에 대한 권장 사항을 제공합니다. 모든 것이 올바르게 작동하는 경우에는 메시지가 표시되지 않으므로 메시지로 귀찮아 할 필요가 없습니다. **Windows** 관리 센터의 **보안** 항목에서도 여전히 컴퓨터의 보안 상태를 살펴볼 수 있습니다.

또한 **Windows** 관리 센터에서는 설치된 프로그램을 관리하고 이러한 프로그램 간에 선택할 수 있는 옵션(예: *설치된 스파이웨어 방지 프로그램 보기*와 같이)도 제공합니다.

관리 센터 설정 변경에서는 경고 메시지를 끌 수도 있습니다(예: *스파이웨어 및 관련 보호에 대한 메시지 끄기*).

9.4.2 Windows 관리 센터와 Avira 제품

네트워크 방화벽

Windows 관리 센터에서 Firewall에 대한 다음 정보를 받을 수 있습니다.

- **Avira FireWall이 켜져 있습니다**
- **Windows 방화벽과 Avira FireWall이 모두 켜져 있습니다.**
- **Windows 방화벽이 꺼져 있거나 올바르게 설정되어 있습니다.**

Avira FireWall이 켜져 있습니다

Avira 제품을 설치하고 나서 Windows 방화벽을 끄면 **관리 센터 > 보안 > 네트워크 방화벽에 Avira FireWall이 현재 켜져 있습니다.**라는 메시지가 표시됩니다. 즉 사용자가 Avira FireWall을 방화벽 솔루션으로 선택했다는 뜻입니다. (Avira FireWall의 대문자 표기에 유의하십시오).

경고

제어판 > **Windows** 방화벽에는 **Avira FireWall**이 아닌 **Windows** 방화벽만 표시됩니다. *방화벽 설정 업데이트와 **Windows** 방화벽 설정이 컴퓨터 보호를 위해 권장되는 설정이 아닙니다.*라는 메시지와 함께 모든 항목에 빨간색 표시가 붙는 이유는 바로 이 때문입니다. 사용자는 아무런 조작도 할 필요가 없으며 Avira 제품이 잘 작동 중이고 PC가 보안 상태입니다.

방화벽 설정 업데이트

Windows 방화벽 설정이 컴퓨터 보호를 위해 권장되는 설정이 아닙니다.

[권장 설정](#)

Windows 방화벽과 Avira FireWall이 모두 켜져 있습니다

Avira FireWall을 비활성화하는 즉시 다음 메시지가 표시됩니다.

네트워크 방화벽 (중요)

Windows 방화벽과 Avira FireWall 둘 다 꺼져 있습니다.

[네트워크 방화벽에 대한 메시지 보기](#)

경고

Avira FireWall을 해제하면 권한이 없는 사용자가 네트워크나 인터넷을 통해 컴퓨터에 액세스할 수도 있습니다.

Windows 방화벽이 꺼져 있거나 올바르게 설정되어 있지 않습니다.
네트워크 방화벽 (중요)

Windows 방화벽이 꺼져 있거나 올바르게 설정되어 있지 않습니다.

[네트워크 방화벽에 대한 메시지 보기](#)

[PC 보호를 위해 온라인으로 앱 찾기](#)

Windows의 Firewall 또는 Avira의 Firewall이 활성화되어 있지 않음을 의미합니다.

• Windows 7에서

Avira FireWall이 올바르게 설정되었거나 올바르게 설치되었습니다. Avira FireWall이 Windows 관리 센터에서 즉시 감지되어야 합니다. 컴퓨터를 다시 부팅하십시오. 그래도 문제가 해결되지 않으면 Avira를 다시 설치하십시오.

바이러스 방지

Windows 관리 센터에서 바이러스 방지에 대한 다음 정보를 받을 수 있습니다.

- Avira Desktop이 최신으로 유지되고 있으며 바이러스 검사 기능이 사용되고 있습니다.
- Avira Desktop이 꺼져 있습니다.
- Avira Desktop이 최신 상태가 아닙니다.
- 이 컴퓨터에서 바이러스 백신 소프트웨어를 찾지 못했습니다.
- Avira Desktop이 만료됐습니다.

Avira Desktop이 최신으로 유지되고 있으며 바이러스 검사 기능이 사용되고 있습니다

Avira 제품 및 후속 업데이트를 설치한 후에는 Windows 관리 센터로부터 어떤 메시지도 표시되지 않습니다. 하지만 **관리 센터 > 보안**으로 이동하면 *Avira Desktop가 최신으로 유지되고 있으며 바이러스 검사 기능이 사용되고 있습니다.*라는 메시지를 볼 수 있습니다. 이는 Avira 제품이 현재 최신 상태이며 Avira Realtime Protection이 사용하도록 설정되어 있음을 의미합니다.

Avira Desktop이 꺼져 있습니다

Avira Real-Time Protection을 사용하지 않도록 설정하거나 Real-Time Protection 서비스를 중지하면 다음 메시지가 표시됩니다.

바이러스 방지 (중요)

Avira Desktop이(가) 꺼져 있습니다.

[바이러스 방지에 대한 메시지 보기](#)

지금 사용(O)

[온라인으로 다른 바이러스 백신 프로그램 가져오기](#)

참고

Avira 제어 센터의 상태에서 Avira Realtime Protection을 사용하거나 사용하지 않도록 설정할 수 있습니다. 작업 표시줄에 빨간색 우산이 퍼져 있으면 AntiVir Real-Time Protection이 활성화되어 있는 것입니다. Windows 관리 센터 메시지에서 *지금 켜기* 버튼을 클릭하여 Avira 제품을 활성화할 수도 있습니다. Avira를 실행해도 되는지 묻는 알림이 표시됩니다. *예, 게시자를 신뢰하고, 프로그램을 실행하겠습니다.*를 클릭하면 Realtime Protection이 다시 사용하도록 설정됩니다.

Avira Desktop이 최신 상태가 아닙니다

Avira을 설치했거나 바이러스 정의 파일, 검사 엔진 또는 보유하고 있는 Avira 제품의 프로그램 파일이 자동 업데이트 되지 않은 경우(예: 기존 Windows 운영 체제에 Avira 제품이 이미 설치된 상태에서 운영 체제를 업그레이드 한 경우), 다음과 같은 메시지를 받게 됩니다.

바이러스 방지 (중요)

Avira Desktop이(가) 최신 상태가 아닙니다.

[바이러스 방지에 대한 메시지 보기](#)

지금 업데이트(U)

[온라인으로 다른 바이러스 백신 프로그램 가져오기](#)

참고
Windows 관리 센터에서 Avira 제품을 최신 상태로 인식하도록 하려면 설치 후 업데이트를 수행해야 합니다. 업데이트를 수행하여 Avira 제품을 업데이트하십시오.

이 컴퓨터에서 바이러스 백신 소프트웨어를 찾지 못했습니다

Windows 관리 센터가 컴퓨터에서 바이러스 백신 소프트웨어를 찾지 못한 경우 Windows 관리 센터에 이 정보가 나타납니다.

바이러스 방지 (중요)

이 컴퓨터에서 바이러스 백신 소프트웨어를 찾지 못했습니다.

[바이러스 방지에 대한 메시지 보기](#)

온라인으로 프로그램 찾기(P)

참고
이 옵션은 Windows Defender가 기본 바이러스 방지 설정 기능을 하는 Windows 8에서는 나타나지 않습니다.

참고
바이러스와 사용자 동의 없이 설치된 기타 프로그램으로부터 컴퓨터를 보호하려면 컴퓨터에 Avira 제품을 설치하여 Avira 제품을 설치하십시오.

Avira Desktop이 만료됐습니다

Avira 제품 라이선스가 만료된 경우 Windows 관리 센터에 이 정보가 나타납니다. 라이선스 갱신 버튼을 클릭하면 신규 라이선스 구매가 가능하도록 Avira 웹사이트로 이동합니다.

<p>바이러스 방지 (중요) Avira Desktop이(가) 더 이상 PC를 보호하지 않습니다. 바이러스 방지에 대한 메시지 보기</p>	<p>조치 취하기(A)</p> <p>설치된 바이러스 백신 앱 보기</p>
---	--

참고
 이 옵션은 Windows 8에서만 사용할 수 있습니다.

스파이웨어 및 사용자 동의 없이 설치된 소프트웨어 보호

Windows 관리 센터에서 스파이웨어 방지에 대한 다음 정보를 받을 수 있습니다.

- [Avira Desktop이 켜져 있습니다.](#)
- [Windows Defender와 Avira Desktop이 모두 켜져 있습니다.](#)
- [Avira Desktop이 최신 상태가 아닙니다.](#)
- [Windows Defender의 상태가 최신이 아닙니다.](#)
- [Windows Defender가 꺼져 있습니다.](#)

Avira Desktop이 켜져 있습니다

Avira 제품 및 후속 업데이트를 설치한 후에는 Windows 관리 센터로부터 어떤 메시지도 표시되지 않습니다. 하지만 [관리 센터 > 보안](#)으로 이동하면 *Avira Desktop이 켜져 있습니다.*를 볼 수 있습니다. 이는 Avira 제품이 현재 최신 상태이며 Avira Realtime Protection이 사용하도록 설정되어 있음을 의미합니다.

Windows Defender와 Avira Desktop이 모두 꺼져 있습니다

Avira Real-Time Protection을 사용하지 않도록 설정하거나 Real-Time Protection 서비스를 중지하면 다음 메시지가 표시됩니다.

<p>스파이웨어 및 원치 않는 소프트웨어 방지 (중요) Windows Defender와 Avira Desktop 둘 다 꺼져 있습니다. 스파이웨어 및 관련 보호에 대한 메시지 보기</p>	<p>스파이웨어 방지 프로그램 보기(S)</p>
---	--

참고
Avira 제어 센터의 상태에서 Avira Realtime Protection을 사용하거나 사용하지 않도록 설정할 수 있습니다. 작업 표시줄에 빨간색 우산이 펼쳐 있으면 AntiVir Real-Time Protection이 활성화되어 있는 것입니다. Windows 관리 센터

메시지에서 *지금 켜기* 버튼을 클릭하여 Avira 제품을 활성화할 수도 있습니다. Avira를 실행해도 되는지 묻는 알림이 표시됩니다. 예, 게시자를 신뢰하고, 프로그램을 실행하겠습니다.를 클릭하면 Realtime Protection이 다시 사용하도록 설정됩니다.

Avira Desktop이 최신 상태가 아닙니다

Avira을 설치했거나 바이러스 정의 파일, 검사 엔진 또는 보유하고 있는 Avira 제품의 프로그램 파일이 자동 업데이트 되지 않은 경우(예: 기존 Windows 운영 체제에 Avira 제품이 이미 설치된 상태에서 운영 체제를 업그레이드 한 경우), 다음과 같은 메시지를 받게 됩니다.

스파이웨어 및 원치 않는 소프트웨어 방지 (중요)

Avira Desktop이(가) 최신 상태가 아닙니다.

[스파이웨어 및 관련 보호에 대한 메시지 보기](#)

지금 업데이트(U)

[온라인으로 다른 스파이웨어 방지 프로그램 가져오기](#)

참고

Windows 관리 센터에서 Avira 제품을 최신 상태로 인식하도록 하려면 설치 후 업데이트를 수행해야 합니다. 업데이트를 수행하여 Avira 제품을 업데이트하십시오.

Windows Defender의 상태가 최신이 아닙니다

Windows Defender가 활성화된 경우 다음 메시지가 표시됩니다. 이미 Avira 제품을 설치한 경우에는 이 메시지가 나타나지 않습니다. 제품이 올바르게 설치되었는지 확인하십시오.

스파이웨어 및 원치 않는 소프트웨어 방지 (중요)

Windows Defender의 상태가 최신이 아닙니다.

[스파이웨어 및 관련 보호에 대한 메시지 보기](#)

지금 업데이트(U)

[온라인으로 다른 스파이웨어 방지 프로그램 가져오기](#)


참고

Windows Defender는 기본 스파이웨어로 Windows의 바이러스 방지 솔루션입니다.

Windows Defender가 꺼져 있습니다

Windows 관리 센터가 컴퓨터에서 운영 체제에 기본으로 통합된 것(Windows Defender) 이외의 다른 바이러스 백신 소프트웨어를 찾지 못한 경우 Windows 관리 센터에 이 정보가 나타납니다. 전에 컴퓨터에 바이러스 백신 소프트웨어를 설치한 경우에는 해당 응용 프로그램이 사용하지 않도록 설정되었습니다. 이미 Avira 제품을 설치했다면 이 메시지가 나타나지 않습니다. Avira 제품이 자동으로 검색됩니다. 제품이 올바르게 설치되었는지 확인하십시오.

스파이웨어 및 원치 않는 소프트웨어 방지 (중요)

 Windows Defender를 사용하도록 설정하지 않았습니다.

[지금 사용\(U\)](#)

[스파이웨어 및 관련 보호에 대한 메시지 보기](#)

[온라인으로 다른 스파이웨어 방지 프로그램 가져오기](#)

10. 바이러스 및 기타

Avira Internet Security은(는) 바이러스 및 맬웨어를 감지할 뿐 아니라 기타 위협으로부터 보호해줍니다. 이 장에서는 다양한 종류의 맬웨어 및 기타 위협의 배경, 동작, 예정되어 있는 불쾌한 놀랄거리에 대해 설명하는 개요를 볼 수 있습니다.

관련 항목:

- [위협 범주](#)
- [바이러스 및 기타 맬웨어](#)

10.1 위협 범주

애드웨어

애드웨어는 컴퓨터 화면에 나타나는 표시줄을 통해 배너 또는 팝업 창을 표시하는 소프트웨어입니다. 일반적으로 이러한 광고는 제거할 수 없어 항상 표시되곤 합니다. 연결 데이터를 통해 사용 동작에 관한 많은 정보를 얻을 수 있어 데이터 보안 측면에서 문제가 됩니다.

Avira 제품은 애드웨어를 검색합니다. [위협 범주](#) 구성에서 선택하여 **애드웨어** 옵션을 사용하도록 설정한 경우(확인 표시 있음) Avira 제품에서 애드웨어가 검색되면 해당하는 알림이 표시됩니다.

애드웨어/스파이웨어

광고를 표시하거나 사용자의 개인 데이터를 당사자 모르게 또는 당사자의 동의 없이 제3자에게 보내는 소프트웨어이며, 따라서 사용자 동의 없이 설치되는 소프트웨어로 간주할 수 있습니다.

Avira 제품은 "애드웨어/스파이웨어"를 인식합니다. [위협 범주](#) 구성에서 선택하여 **애드웨어/스파이웨어** 옵션을 사용하도록 설정한 경우(확인 표시 있음) Avira 제품에서 애드웨어나 스파이웨어가 검색되면 해당하는 알림이 표시됩니다.

응용 프로그램

APPL은 사용할 경우 위험을 초래할 수 있거나 출처가 의심스러운 각각의 응용 프로그램을 가리킵니다.

Avira 제품은 "APPL(애플리케이션)"을 인식합니다. [위협 범주](#) 구성에서 선택하여 **애플리케이션** 옵션을 사용하도록 설정한 경우(확인 표시 있음) Avira 제품에서 이러한 동작이 검색되면 해당하는 알림이 표시됩니다.

백도어 클라이언트

사용자 몰래 컴퓨터에 설치되어 데이터를 유출하거나 컴퓨터를 조작하는 프로그램을 백도어 서버 프로그램이라고 합니다. 이 프로그램은 제3자가 인터넷이나 네트워크를 통해 백도어 제어 소프트웨어(클라이언트)를 사용하여 제어할 수 있습니다.

Avira 제품은 "백도어 제어 소프트웨어"를 인식합니다. **위험 범주** 구성에서 선택하여 **백도어 제어 소프트웨어** 옵션을 사용하도록 설정한 경우(확인 표시 있음) Avira 제품에서 그러한 소프트웨어가 검색되면 해당하는 알림이 표시됩니다.

다이얼러

인터넷에서 제공하는 일부 서비스는 유료입니다. 독일의 경우 0190/0900 번호의 다이얼러에서 요금이 부과됩니다. 오스트리아 및 스위스에서는 09x0이고 독일에서는 중반기에 09x0으로 바뀔 예정입니다. 이러한 프로그램이 컴퓨터에 설치되면 해당 프리미엄 요금제 번호를 통한 연결이 보장되는데, 요금에 큰 차이가 있을 수 있습니다.

전화 요금 고지서를 통한 온라인 콘텐츠 마케팅은 합법적이며 사용자에게 유익할 수 있습니다. 정품 다이얼러는 사용자가 목적에 따라 의도적으로 사용하므로 위험할 여지가 없습니다. 이러한 다이얼러는 명확하고 확실히 표시되는 레이블 또는 요청을 통해 사용자가 동의한 경우에만 사용자의 컴퓨터에 설치됩니다. 정품 다이얼러의 전화 접속 프로세스는 명확하게 표시됩니다. 게다가 정품 다이얼러에서는 발생한 요금을 착오 없이 정확하게 알려 줍니다.

그러나 의심스러운 수단을 통해 또는 속이려는 의도로 사용자 모르게 컴퓨터에 설치되는 다이얼러도 있습니다. 예를 들어, 인터넷 사용자의 기본 ISP(Internet Service Provider) 데이터 통신 링크를 바꿔 놓고 연결이 설정될 때마다 유료 번호, 종종 엄청나게 비싼 0190/0900 번호로 전화를 걸게 합니다. 사용자는 전화요금 고지서를 받아볼 때까지는 자신의 컴퓨터에 설치된 0190/0900 다이얼러 프로그램이 연결할 때마다 프리미엄 요금제 번호로 전화를 걸어 통신 요금이 크게 늘어났다는 사실을 알아채기가 어렵습니다.

전화 서비스 공급자에게 직접 연락해 그 번호 범위를 차단하도록 요청함으로써 사용자 동의 없이 설치되는 다이얼러(0190/0900 다이얼러)로부터 더 이상 피해를 입지 않게 하십시오.

Avira 제품에서는 대표적인 다이얼러를 기본적으로 검색할 수 있습니다.

위험 범주 구성에서 선택하여 **다이얼러** 옵션이 사용하도록 설정한 경우(확인 표시 있음) 다이얼러가 검색되면 해당하는 알림이 표시됩니다. 이제 사용자 동의 없이 설치되었을 0190/0900 다이얼러를 간단하게 삭제할 수 있습니다. 그러나 사용자가 동의하여 설치된 전화 접속 프로그램인 경우 이를 예외 파일로 선언하면 앞으로 더 이상 검사하지 않습니다.

이중 확장명 파일

실제 파일 확장명을 의심스럽게 숨긴 실행 파일입니다. 이러한 위장 방법은 맬웨어에서 종종 사용됩니다.

Avira 제품은 "이중 확장명 파일"을 인식합니다. **위협 범주** 구성에서 선택하여 **이중 확장명 파일** 옵션을 사용하도록 설정한 경우(확인 표시 있음) Avira 제품에서 그러한 파일이 검색되면 해당하는 알림이 표시됩니다.

사기성 소프트웨어

"스캐어웨어" 또는 "로그웨어"라고도 하며, 사용자의 컴퓨터가 바이러스 또는 맬웨어에 감염된 것처럼 보이게 하는 사기성 소프트웨어입니다. 이 소프트웨어는 전문 바이러스 백신 소프트웨어하게 보이지만 불확실성 높거나 사용자에게 겁을 주기 위한 수단입니다. 이 소프트웨어는 사용자가 (가공의) 임박한 위협에 두려움을 느끼고 이를 해결하기 위해 비용을 지불하도록 하는 데 목적이 있습니다. 또한 피해자로 하여금 공격을 받았다고 믿게 만들어 어떤 작업을 수행하도록 지시하는 경우도 있습니다. 실제로는 그 작업을 수행함으로써 공격을 받게 됩니다.

Avira 제품은 스캐어웨어를 검색합니다. **위협 범주** 구성에서 선택하여 **사기성 소프트웨어**를 사용하도록 설정한 경우(확인 표시 있음) Avira 제품에서 이러한 파일이 검색되면 해당하는 알림이 표시됩니다.

게임

컴퓨터 게임을 즐겨도 괜찮은 곳이 있습니다. 그러나 (아마도 점심 시간을 제외하고) 직장은 해당되지 않을 것입니다. 그럼에도 불구하고 회사 직원 및 공무원들이 인터넷에서 다운로드할 수 있는 수많은 게임, 지리찾기, **Patience** 등을 즐기곤 합니다. 인터넷에서 온갖 종류의 게임을 다운로드할 수 있습니다. 전자 메일 게임의 인기도 점점 높아지고 있습니다. 간단한 체스 게임부터 "함대 훈련"(어뢰 전투 포함)에 이르기까지 다양한 게임이 유포되고 있습니다. 해당하는 링크가 전자 메일 프로그램을 통해 파트너에게 전송되면, 이들은 이러한 메일에 회신합니다.

조사에 따르면, 업무 중에 컴퓨터 게임에 보내는 시간이 미치는 경제적 영향은 이미 오래 전부터 상당한 수준에 이르렀습니다. 따라서 점점 더 많은 기업들이 업무용 컴퓨터에서 컴퓨터 게임을 금지하는 방법을 모색하고 있습니다.

Avira 제품은 컴퓨터 게임을 인식합니다. **위협 범주** 구성에서 선택하여 **게임** 옵션을 사용하도록 설정한 경우(확인 표시 있음) Avira 제품에서 게임이 검색되면 해당하는 알림이 표시됩니다. 이제 간단하게 삭제할 수 있으므로, 진정한 의미로 게임은 끝난 것입니다.

장난 프로그램

장난 프로그램은 피해를 주거나 복제되는 일 없이 누군가를 놀라게 하거나 재미를 선사하는 데 목적이 있습니다. 장난 프로그램이 로드된 컴퓨터는 특정 시점에 어떤 멜로디를 재생하거나 이상한 화면을 표시합니다. 예를 들면, 디스크 드라이브의 세탁기(DRAIN.COM) 또는 화면을 차지하는 프로그램(BUGSRES.COM)이 있습니다.

그러나 조심하십시오. 장난 프로그램의 모든 증상이 바이러스 또는 트로이 목마에서 비롯되었을 수도 있습니다. 적어도 사용자가 너무 놀라거나 당황한 나머지 화를 자초할 수도 있습니다.

Avira 제품은 광범위한 검사 및 식별 루틴을 통해 장난 프로그램을 검색하고, 필요하다면 이를 사용자 동의 없이 설치된 프로그램으로 간주하여 제거할 수 있습니다. **위협 범주** 구성에서 **장난 프로그램** 옵션을 사용하도록 설정한 경우(확인 표시 있음) 장난 프로그램이 검색되면 해당하는 알림이 표시됩니다.

피싱

"브랜드 스푸핑"이라고도 하는 피싱은 인터넷 서비스 공급자, 은행, 온라인 बैं킹 서비스, 등록 기관 등의 고객 또는 잠재 고객을 겨냥하는, 지능적인 데이터 도용 수법입니다. 인터넷을 통해 전자 메일 주소를 제출하거나, 온라인 양식을 작성하거나, 뉴스 그룹 또는 웹사이트에 액세스할 때 "인터넷을 배회하는 도용자"가 데이터를 훔쳐서 사용자의 허락 없이 사기 또는 기타 범죄 행위에 사용할 수 있습니다.

Avira 제품은 "피싱"을 인식합니다. **위협 범주** 구성에서 선택하여 **피싱** 옵션을 사용하도록 설정한 경우(확인 표시 있음) Avira 제품에서 이러한 동작이 검색되면 해당하는 알림이 표시됩니다.

개인 도메인을 위반한 프로그램

시스템의 보안을 손상시킬 소지가 있는 소프트웨어는 사용자 동의 없이 설치된 프로그램의 활동을 개시하거나 개인 정보를 유출하거나 사용자의 동작을 염탐하므로 이 역시 사용자 동의 없이 설치되는 것으로 간주할 수 있습니다.

Avira 제품에서는 "Security Privacy Risk" 소프트웨어를 검색합니다. **위협 범주** 구성에서 선택하여 **개인 도메인을 위반한 프로그램**을 사용하도록 설정한 경우(확인 표시 있음) Avira 제품에서 이러한 소프트웨어가 검색되면 해당하는 알림이 표시됩니다.

비정상적인 런타임 압축 프로그램

비정상적인 런타임 압축 도구로 압축된 파일은 의심스러운 파일로 분류될 수 있습니다.

Avira 제품에서는 "비정상적인 런타임 압축 프로그램"을 인식합니다. **위협 범주** 구성에서 선택하여 **비정상적인 런타임 압축 프로그램** 옵션을 사용하도록 설정한 경우(확인 표시 있음) Avira 제품에서 이러한 압축 프로그램이 검색되면 해당하는 알림이 표시됩니다.

10.2 바이러스 및 기타 맬웨어

애드웨어

애드웨어는 컴퓨터 화면에 나타나는 표시줄을 통해 배너 또는 팝업 창을 표시하는 소프트웨어입니다. 일반적으로 이러한 광고는 제거할 수 없어 항상 표시되곤 합니다. 연결 데이터를 통해 사용 동작에 관한 많은 정보를 얻을 수 있어 데이터 보안 측면에서 문제가 됩니다.

백도어

백도어는 컴퓨터 액세스 보안 메커니즘을 우회하여 컴퓨터에 액세스할 수 있습니다.

백그라운드에서 실행 중인 프로그램은 사이버 범죄자에게 거의 무제한의 권한을 부여할 수 있습니다. 백도어를 통해 사용자의 개인 데이터를 훔칠 수 있습니다. 하지만 주로 해당 시스템에 다른 컴퓨터 바이러스나 웜을 설치하는 데 이용됩니다.

부트 바이러스

하드 디스크의 부트 또는 마스터 부트 섹터는 주로 부트 섹터 바이러스에 감염됩니다. 부트 섹터 바이러스는 시스템을 실행하는 데 필요한 중요 정보를 덮어씁니다. 그 결과 컴퓨터 시스템이 더 이상 로드되지 않을 수 있습니다.

봇넷

봇넷은 (인터넷상의) 원격 PC 네트워크로서 상호 통신하는 봇들로 구성됩니다. 봇넷은 일반 명령 및 제어 인프라를 통해 프로그램(일반적으로 웜, 트로이 목마라고 함)을 실행하는 일련의 감염된 시스템으로 구성될 수 있습니다. 봇넷은 DoS(Denial-of-Service)를 비롯한 다양한 목적으로 쓰이며, 감염된 PC 사용자가 미처 인식하지 못할 수도 있습니다. 봇넷의 주된 위험성은 네트워크가 수천 대의 컴퓨터로 확장되어 총 대역폭이 일반적인 인터넷 액세스를 초과할 수 있다는 점입니다.

Exploit

Exploit(보안 취약점)는 버그, 결함 또는 취약점을 이용하여 컴퓨터 시스템에 대한 권한 상승 또는 DoS를 유발하는 컴퓨터 프로그램 또는 스크립트입니다. 예를 들어 Exploit의 한 가지 형식은 조작된 데이터 패키지를 통한 인터넷으로부터의 공격입니다. 더 높은 액세스 권한을 얻기 위해 프로그램에 침투할 수 있습니다.

사기성 소프트웨어

"스캐어웨어" 또는 "로그웨어"라고도 하며, 사용자의 컴퓨터가 바이러스 또는 맬웨어에 감염된 것처럼 보이게 하는 사기성 소프트웨어입니다. 이 소프트웨어는 전문 바이러스 백신 소프트웨어하게 보이지만 불확실성 높거나 사용자에게 겁을 주기 위한 수단입니다. 이 소프트웨어는 사용자가 (가공의) 임박한 위험에 두려움을 느끼고 이를 해결하기 위해 비용을 지불하도록 하는 데 목적이 있습니다. 또한 피해자로 하여금 공격을 받았다고 믿게 만들어 어떤 작업을 수행하도록 지시하는 경우도 있습니다. 실제로는 그 작업을 수행함으로써 공격을 받게 됩니다.

혹스(Hoaxes)

몇 년 전부터 인터넷 및 기타 네트워크 사용자들에게 전자 메일을 통해 유포되었다는 바이러스에 관한 알림 메시지가 전달되곤 했습니다. 이러한 경고는 사용자에게 "위험"에 대해 경고하기 위해 가능한 한 많은 동료 또는 다른 사용자에게 전송하라는 요청을 포함한 전자 메일로 전파됩니다.

허니팟

허니팟(Honeypot)은 네트워크에 설치된 서비스(프로그램 또는 서버)입니다. 네트워크를 모니터하고 공격을 로그합니다. 이 서비스는 합법적인 사용자에게 알려지지 않으며, 따라서 사용자의 주소가 지정되지 않습니다. 공격자가 네트워크의 취약점을 찾고 허니팟에서 제공하는 서비스를 이용할 경우, 로그에 기록되고 알림이 발효됩니다.

매크로 바이러스

매크로 바이러스는 응용 프로그램의 매크로 언어(예: WinWord 6.0의 WordBasic)로 작성되어 이 응용 프로그램 문서에서만 확산될 수 있는 작은 프로그램입니다. 따라서 문서 바이러스라고도 합니다. 매크로 바이러스가 활성화되려면 해당 응용 프로그램이 활성화되고 감염된 매크로 중 하나가 실행되어야 합니다. "일반" 바이러스와 달리 매크로 바이러스는 실행 파일을 공격하지 않고 해당 호스트 응용 프로그램의 문서를 공격합니다.

파밍

파밍은 웹 브라우저의 호스트 파일을 수정하여 쿼리가 스푸핑된 웹 사이트로 전달되게 합니다. 이는 고전적인 피싱 수법에서 발전된 형태입니다. 파밍 수법을 구사하는 자들은 가짜 웹 사이트가 저장된 대규모 서버 팜을 자체적으로 운영합니다. 파밍은 다양한 DNS 공격 유형을 아우르는 용어로 쓰이고 있습니다. 호스트 파일을 수정하는 경우, 트로이 목마 또는 바이러스를 이용하여 시스템을 수정하곤 합니다. 그로 인해 올바른 웹 주소를 입력하더라도 해당 시스템은 가짜 웹 사이트에만 액세스하게 됩니다.

피싱

피싱은 인터넷 사용자의 개인 정보를 빼내는 행위를 의미합니다. 일반적으로 피싱 수법에서는 공식 서한처럼 보이는 전자 메일 등을 피해자들에게 보내서 기밀 정보(특히 온라인 banking 계정의 사용자 이름, 암호, **PIN, TAN** 등)를 공개하게끔 유도합니다. 이렇게 훔쳐낸 액세스 정보를 이용하여 그 피해자의 신분을 알아내고 이 신분으로 거래를 수행합니다. 은행 및 보험사는 절대 전자 메일, **SMS** 또는 전화를 통해 신용카드 번호, **PIN, TAN** 또는 기타 액세스 정보를 요청하지 않습니다.

다형성 바이러스

다형성 바이러스는 위장의 귀재입니다. 자체 프로그래밍 코드를 바꾸므로 찾아내기가 매우 어렵습니다.

프로그램 바이러스

컴퓨터 바이러스는 실행된 후 다른 프로그램에 첨부되어 감염시킬 수 있는 프로그램입니다. 이 바이러스는 논리 폭탄(지발형 바이러스)이나 트로이 목마와 달리 스스로 증식됩니다. 웜과는 대조적으로 바이러스는 악성 코드로 사용할 호스트 프로그램이 필요합니다. 호스트 프로그램 자체가 실행된다는 규칙은 바뀌지 않습니다.

Rootkits

Rootkits는 침입을 받은 컴퓨터 시스템에 설치되는 소프트웨어 도구 모음으로, 자신을 숨기기 위해 침입자의 로그인을 은폐하고 프로세스를 숨기며 데이터를 기록합니다. 이미 설치된 스파이 프로그램을 업데이트하고 삭제된 스파이웨어를 다시 설치하려고 시도합니다.

스크립트 바이러스 및 웜

이러한 바이러스는 매우 쉽게 프로그래밍할 수 있으므로, 필요한 기술만 있다면 전자 메일을 통해 불과 몇 시간 만에 전 세계에 확산될 수 있습니다.

스크립트 바이러스 및 웜은 **Javascript, VBScript**와 같은 스크립트 언어를 이용하여 다른 새로운 스크립트에 침투하거나 운영 체제 기능을 호출하여 유포됩니다. 주로 전자 메일 또는 파일(문서)을 주고 받는 과정에서 종종 발생합니다.

웜은 자체적으로 증식되지만 호스트를 감염시키지는 않는 프로그램입니다. 따라서 웜은 다른 프로그램 시퀀스에 포함되지 않습니다. 주로 웜은 보안 수단이 제한된 시스템에 유해 프로그램을 침투시키는 역할만 담당합니다.

스파이웨어

스파이웨어는 사용자의 명시적인 동의 없이 컴퓨터 작업을 가로채거나 부분적으로 제어하는 스파이 프로그램입니다. 스파이웨어는 감염된 컴퓨터를 이용해 금전적 이익을 얻기 위해 만들어집니다.

트로이 목마(약어: 트로이)

현재 트로이는 매우 일반적인 바이러스입니다. 특정 기능이 있는 것처럼 가장하지만, 실행된 후에 실제 이미지를 표시하고 대부분의 경우 파괴적인 다른 기능을 수행하는 이 프로그램이 트로이에 포함됩니다. 트로이 목마는 자가 증식할 수 없다는 특징으로 바이러스 및 웜과 구별됩니다. 대부분의 트로이 목마는 사용자가 트로이 목마를 실행하도록 하기 위해 흥미를 끄는 이름(**SEX.EXE** 또는 **STARTME.EXE**)이 붙어 있습니다. 실행 직후 활성화되어 하드 디스크를 포맷하는 등의 작업을 수행할 수 있습니다. 드로퍼(**dropper**)는 특수한 형태의 트로이 목마로서 바이러스를 '투하'합니다. 즉 바이러스가 컴퓨터 시스템에 내장되게 합니다.

좀비

좀비 **PC**는 맬웨어 프로그램에 감염된 컴퓨터이며 해커가 해당 컴퓨터를 원격으로 제어하여 범죄에 이용할 수 있습니다. 감염된 **PC**는 해커의 명령에 따라 **DoS** 공격을 개시하거나 스팸 및 피싱 전자 메일을 보냅니다.

11. 정보 및 서비스

이 장에서는 Avira에 문의하는 방법을 안내합니다.

- 참조:[연락처 주소](#)
- 참조:[기술 지원](#)
- 참조:[의심스러운 파일](#)
- 참조:[오진 보고](#)
- 참조:[보안 강화를 위한 사용자 의견 보내기](#)

11.1 연락처 주소

Avira 제품군에 대해 궁금한 사항이나 요청 사항이 있을 경우 언제든지 문의해 주십시오. 연락처 주소는 [도움말 > Avira Internet Security 정보](#)를 참조하십시오.

11.2 기술 지원

Avira 지원 부서에서는 고객의 질문 또는 기술적 문제를 해결할 수 있도록 신뢰할 만한 서비스를 제공합니다.

Avira의 포괄적인 지원 서비스에 대한 모든 정보는 웹 사이트에서 확인하실 수 있습니다.

<http://www.avira.kr/premium-suite-support>

빠르고 안정적인 지원을 제공할 수 있도록 다음 정보를 미리 준비해 주십시오.

- **라이선스 정보.** 이 정보는 프로그램 인터페이스의 메뉴 항목 [도움말 > Avira Internet Security 정보 > 라이선스 정보](#)에서 찾을 수 있습니다. 라이선스 정보를 참조하십시오.
- **버전 정보.** 이 정보는 프로그램 인터페이스의 메뉴 항목 [도움말 > Avira Internet Security 정보 > 버전 정보](#)에서 찾을 수 있습니다. 버전 정보를 참조하십시오.
- 설치된 운영 체제 버전 및 모든 서비스 팩
- 설치된 소프트웨어 패키지(예: 다른 공급업체의 바이러스 백신 소프트웨어)
- 프로그램 또는 보고서 파일의 **정확한 메시지**

11.3 의심스러운 파일

제품에서 검색하거나 제거할 수 없는 바이러스 또는 의심스러운 파일은 Avira에 보내 주십시오. 몇 가지 방법을 통해 보내실 수 있습니다.

- Avira Server Security Console 제어 센터의 격리 관리자에서 파일을 확인하고 상황에 맞는 메뉴 또는 해당 버튼을 사용하여 **파일 보내기** 항목을 선택합니다.
- 압축된 파일(WinZIP, PKZip, Arj 등)을 전자 메일에 첨부하여 다음 주소로 전송합니다: virus-premium-suite@avira.kr
일부 전자 메일 게이트웨이에서는 바이러스 백신 소프트웨어가 작동하므로 파일에 암호를 지정해야 합니다(반드시 암호를 알려 주십시오.).
- 의심스러운 파일을 웹 사이트(<http://www.avira.kr/sample-upload>)를 통해 전송할 수도 있습니다.

11.4 오진 보고

Avira 제품에서 검색된 항목이 있다고 보고한 파일이 "깨끗한" 파일일 가능성이 매우 크다고 생각되는 경우, 해당 파일을 압축(WinZIP, PKZip, Arj 등)하고 전자 메일에 첨부하여 다음 주소로 보내 주십시오.

virus-premium-suite@avira.kr

일부 전자 메일 게이트웨이에서는 바이러스 백신 소프트웨어와 연동하므로 파일과 함께 암호도 제공해야 합니다. 반드시 암호를 알려 주십시오.

11.5 보안 강화를 위한 사용자 의견 보내기

Avira는 고객의 보안을 무엇보다 중요하게 생각합니다. 따라서 Avira는 제품 출시 전에 모든 Avira 솔루션의 품질과 보안을 테스트하는 자체 전문팀을 운영하고 있습니다. 또한 발생 가능한 보안 관련 간격에 관련한 징후도 중요하게 여기며 이를 신중하게 처리합니다.

Avira 제품에서 보안 허점을 발견한 경우 다음 주소로 전자 메일을 보내 주십시오.

vulnerabilities-premium-suite@avira.kr

12. 참조: 구성 옵션

구성 참조는 사용할 수 있는 모든 구성 옵션을 문서화합니다.

12.1 Scanner

구성의 **Scanner** 섹션에서는 수동 검사를 구성합니다. (옵션은 고급 모드에서만 사용 가능)

12.1.1 검사

수동 검사 루틴 동작을 정의할 수 있습니다(고급 모드에서만 사용 가능). 검사할 특정 디렉터리를 선택하는 경우 구성에 따라 **Scanner**에서 다음과 같이 검사합니다.

- 특정 우선 순위를 적용하여 검사
- 부트 섹터와 주 메모리 검사
- 디렉터리의 모든 파일 또는 선택한 파일 검사

파일

Scanner에서는 필터를 사용하여 특정 확장명(형식)이 지정된 파일만 검사할 수 있습니다.

모든 파일

이 옵션을 선택하면 파일 콘텐츠와 파일 확장명에 관계없이 모든 파일을 대상으로 바이러스와 사용자 동의 없이 설치된 프로그램을 검사합니다. 필터가 사용되지 않습니다.

참고

모든 파일을 사용하는 경우 **파일 확장명** 버튼을 선택할 수 없습니다.

스마트 확장명 사용

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 있는지 검사할 파일이 자동으로 선택됩니다. 즉, **Avira** 프로그램에서 파일 콘텐츠에 따라 파일을 검사할지 여부를 결정합니다. 이 절차는 **파일 확장명 목록 사용**보다는 다소 느리지만 파일 확장명만을 기준으로 검사하지 않으므로 더 정확합니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

참고

스마트 확장명 사용을 사용하면 **파일 확장명** 버튼을 선택할 수 없습니다.

파일 확장명 목록 사용

이 옵션을 사용하면 지정된 확장명의 파일만 검사합니다. 바이러스와 사용자 동의 없이 설치된 프로그램을 포함할 수 있는 모든 파일 형식이 미리 설정되어 있습니다. 이 목록은 "파일 확장명" 버튼을 통해 수동으로 편집할 수 있습니다.

참고

이 옵션을 사용하고 파일 확장명 목록에서 모든 항목을 삭제한 경우 **파일 확장명** 버튼 아래에 "파일 확장명 없음"이라는 텍스트가 표시됩니다.

파일 확장명

이 버튼을 사용하면 대화 상자 창이 열리고 이 창에 "파일 확장명 목록 사용" 모드에서 검사될 모든 파일 확장명이 표시됩니다. 확장명에 대한 기본 항목이 설정되어 있지만 항목을 추가하거나 삭제할 수 있습니다.

참고

기본 목록은 버전마다 다를 수 있습니다.

추가 설정

선택한 드라이브의 부트 섹터 검사

이 옵션을 사용하면 **Scanner**에서 시스템 검사용으로 선택된 드라이브의 부트 섹터만 검사합니다. 이 옵션은 기본 설정으로 선택됩니다.

마스터 부트 섹터 검사

이 옵션을 사용하면 **Scanner**에서 시스템에 사용된 하드 디스크의 마스터 부트 섹터를 검사합니다.

오프라인 파일 무시

이 옵션을 사용하면 직접 검사에서 검사 시 오프라인 파일을 완전히 무시합니다. 따라서 이러한 파일에 대해서는 바이러스나 사용자 동의없이 설치된 프로그램의 포함 여부를 검사하지 않습니다. 오프라인 파일은 **HSMS**(계층 저장소 관리 시스템)를 통해 하드 디스크에서 테이프 같은 미디어로 실제 이동된 파일을 말합니다. 이 옵션은 기본 설정으로 선택됩니다.

시스템 파일에 대한 무결성 확인

이 옵션을 사용하면 수동 검사에서 가장 중요한 **Windows** 시스템 파일에 대해 맬웨어에 의한 변경 여부를 확인하는 특수 보안 검사가 실시됩니다. 수정된 파일이 발견되면 의심스러운 항목으로 보고됩니다. 이 기능에는 컴퓨터 용량이 많이 사용됩니다. 이 옵션은 기본적으로 사용되지 않습니다.

참고

이 옵션은 Windows Vista 이상에서만 사용할 수 있습니다.

참고

시스템 파일을 수정하고 부팅 또는 시작 화면을 사용자 고유의 요구 사항에 맞게 조정하는 타사 도구를 사용하는 경우에는 이 옵션을 사용하지 마십시오. 이러한 도구의 예로는 **skinpacks**, **TuneUp utilities** 또는 **Vista Customization** 등이 있습니다.

최적화된 검사

이 옵션을 사용하면 **Scanner** 검사 시 프로세서 용량 활용이 최적화됩니다. 성능상의 이유로 최적화된 검사는 표준 수준에서만 기록됩니다.

참고

이 옵션은 다중 프로세서 시스템에서만 사용할 수 있습니다.

기호 링크로 이동

이 옵션을 사용하면 **Scanner**에서 검사 프로파일 또는 선택한 디렉터리의 모든 기호 링크를 따라가 연결된 파일에 대해 바이러스 및 맬웨어 포함 여부를 검사하는 방식으로 검사를 수행합니다.

참고

이 옵션은 바로 가기를 포함하지 않지만 파일 시스템에서 투명한 기호 링크(**mklink.exe**를 통해 생성됨) 또는 연결 지점(**junction.exe**를 통해 생성됨)만을 참조합니다.

검사 전 Rootkits 검색

이 옵션을 사용하는 상태에서 검사를 시작하면 **Scanner**에서 Windows 시스템 디렉터리에 대해 바로 가기에 활성 **Rootkits**가 있는지 검사합니다. 이 프로세스는 "**Rootkits 검사**" 검사 프로파일만큼 포괄적으로 컴퓨터에 대해 활성 **Rootkits**를 검사하지 않지만, 수행 속도가 상당히 빠릅니다. 이 옵션은 사용자가 만든 프로파일의 설정만 변경합니다.

참고

Windows XP 64비트

레지스트리 검사

이 옵션을 사용하면 레지스트리에서 맬웨어 참조를 검사합니다. 이 옵션은 사용자가 만든 프로필의 설정만 변경합니다.

네트워크 드라이브의 파일 및 경로 무시

이 옵션을 사용하면 컴퓨터에 연결된 네트워크 드라이브가 수동 검사에서 제외됩니다. 이 옵션은 서버 또는 다른 워크스테이션이 바이러스 백신 소프트웨어로 자체 보호되는 경우에 사용하는 것이 좋습니다. 이 옵션은 기본적으로 사용되지 않습니다.

검사 프로세스

Scanner 중지 허용

이 옵션을 사용하면 "Luke Filewalker" 창의 "중지" 버튼을 사용하여 바이러스나 사용자 동의 없이 설치된 프로그램에 대한 검사를 언제든지 종료할 수 있습니다. 이 설정을 사용하지 않는 경우에는 "Luke Filewalker" 창에 중지 버튼이 회색으로 표시됩니다. 따라서 검사 프로세스를 조기에 종료할 수 없습니다! 이 옵션은 기본 설정으로 선택됩니다.

Scanner 우선 순위

수동 검사 시 Scanner에서는 우선 순위를 구분합니다. 몇 개 프로세스가 워크스테이션에서 동시에 실행 중인 경우에만 적용됩니다. 선택에 따라 검사 속도가 달라집니다.

낮음

다른 프로세스에서 계산 시간을 필요로 하지 않는 경우에만 운영 체제에서 Scanner에 프로세서 시간을 할당합니다. 따라서 Scanner가 최저 속도로 실행됩니다. 대체로 다른 프로그램과의 작업을 우선으로 합니다. 다른 프로그램에서 계산 시간을 필요로 하는 동안 Scanner가 백그라운드에서 계속 실행되는 경우 컴퓨터가 더 빨리 응답합니다.

보통

Scanner가 보통의 우선 순위로 실행됩니다. 운영 체제에서 모든 프로세스에 동일한 양의 프로세서 시간을 할당합니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다. 특수한 경우 다른 응용 프로그램과의 작업에 영향이 미칠 수도 있습니다.

높음

Scanner에 최고 우선 순위가 부여됩니다. 다른 응용 프로그램과의 동시 작업이 거의 불가능합니다. 하지만 Scanner가 최고 속도로 검사를 수행합니다.

검색 시 작업

Scanner에서 바이러스나 사용자 동의 없이 설치된 프로그램을 발견했을 때 수행할 작업을 정의할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

대화형

이 옵션을 사용하면 **Scanner**의 검사 결과가 대화 상자에 표시됩니다. **Scanner**을 사용하여 검사를 수행할 경우 검사가 완료되면 영향받는 파일 목록과 함께 알림이 제공됩니다. 콘텐츠별 메뉴를 사용하여 감염된 여러 파일에 대해 실행할 작업을 선택할 수 있습니다. 감염된 모든 파일에 대해 표준 작업을 실행하거나 **Scanner**를 취소할 수 있습니다.

참고

격리는 **Scanner** 알림에 기본적으로 선택되어 있습니다. 상황에 맞는 메뉴를 통해 추가 작업을 선택할 수 있습니다.

자동

이 옵션을 사용하면 바이러스가 검색되어도 대화 상자가 표시되지 않습니다. **Scanner**는 이 섹션에서 기본 및 보조 작업으로 미리 정의하는 설정에 따라 작동합니다.

작업 전에 격리 저장소로 복사

이 옵션을 사용하면 **Scanner**에서 요청한 기본 작업 또는 보조 작업을 수행하기 전에 백업 복사본을 만듭니다. 백업 복사본은 격리 저장소에 저장되는데, 격리 저장소에서는 파일에 정보 값이 있는 경우 파일을 복원할 수 있습니다. 또한 추가 조사를 위해 백업 복사본을 Avira 맬웨어 연구 센터로 보낼 수도 있습니다.

기본 작업

기본 작업은 **Scanner**에서 바이러스나 사용자 동의 없이 설치된 프로그램을 발견한 경우에 수행하는 작업입니다. "복구" 옵션을 선택했지만 영향받는 파일을 복구할 수 없는 경우 "보조 작업"에 선택된 작업이 수행됩니다.

참고

기본 작업 아래에서 복구 설정을 선택한 경우에만 **보조 작업** 옵션을 선택할 수 있습니다.

복구

이 옵션을 사용하면 **Scanner**에서 영향받는 파일을 자동으로 복구합니다. 영향받는 파일을 복구할 수 없는 경우 **Scanner**에서는 **보조 작업**에 선택된 작업을 수행합니다.

참고

자동 복구를 사용하는 것이 좋지만, 이 경우 **Scanner**에서 워크스테이션의 파일을 수정하게 됩니다.

이름 바꾸기

이 옵션을 사용하면 **Scanner**에서 파일 이름을 바꿉니다. 따라서 더블클릭과 같은 방법으로 이러한 파일에 더 이상 직접 액세스할 수 없습니다. 파일을 나중에 복구하고 원래 이름을 다시 지정할 수 있습니다.

격리 저장소

이 옵션을 사용하면 **Scanner**에서 파일을 격리 저장소로 옮깁니다. 이러한 파일은 나중에 복구하거나 필요할 경우 **Avira** 맬웨어 연구 센터로 보낼 수 있습니다.

삭제

이 옵션을 사용하면 파일이 삭제됩니다. 이 프로세스는 "덮어쓰기 및 삭제"보다 훨씬 빠릅니다.

무시

이 옵션을 사용하면 파일에 액세스할 수 있고 파일이 그대로 유지됩니다.

경고

영향받는 파일은 워크스테이션에서 활성 상태로 유지됩니다. 이로 인해 워크스테이션에 심각한 손상이 발생할 수 있습니다.

덮어쓰기 및 삭제

이 옵션을 사용하면 **Scanner**에서 파일을 기본 패턴으로 덮어쓴 다음 삭제합니다. 이 파일은 복원할 수 없습니다.

보조 작업

"기본 작업" 아래에서 복구 설정을 선택한 경우에만 "보조 작업" 옵션을 선택할 수 있습니다. 이 옵션을 사용하면 영향받는 파일을 복구할 수 없는 경우 해당 파일에 대해 수행할 작업을 결정할 수 있습니다.

이름 바꾸기

이 옵션을 사용하면 **Scanner**에서 파일 이름을 바꿉니다. 따라서 더블클릭과 같은 방법으로 이러한 파일에 더 이상 직접 액세스할 수 없습니다. 파일을 나중에 복구하고 원래 이름을 다시 지정할 수 있습니다.

격리 저장소

이 옵션을 사용하면 **Scanner**에서 파일을 격리 저장소로 옮기니다. 이러한 파일은 나중에 복구하거나 필요할 경우 **Avira** 맬웨어 연구 센터로 보낼 수 있습니다.

삭제

이 옵션을 사용하면 파일이 삭제됩니다. 이 프로세스는 "덮어쓰기 및 삭제"보다 훨씬 빠릅니다.

무시

이 옵션을 사용하면 파일에 액세스할 수 있고 파일이 그대로 유지됩니다.

경고

영향받는 파일은 워크스테이션에서 활성 상태로 유지됩니다. 이로 인해 워크스테이션에 심각한 손상이 발생할 수 있습니다.

덮어쓰기 및 삭제

이 옵션을 사용하면 **Scanner**에서 파일을 기본 패턴으로 덮어쓰는 다음 삭제합니다. 이 파일은 복원할 수 없습니다.

참고

삭제나 덮어쓰기 및 삭제를 기본 또는 보조 작업으로 선택한 경우 추론(heuristic) 적중 시 영향받는 파일이 삭제되지 않고 격리 보관소로 이동됩니다.

압축파일

압축파일을 검사할 때 **Scanner**에서는 재귀 검사를 사용합니다. 즉, 압축파일 안에 들어 있는 압축파일도 압축을 풀어서 바이러스나 사용자 동의 여부와 관계 없이 설치된 프로그램이 있는지 검사합니다. 파일을 검사하고 나서 압축을 풀어서 파일을 다시 검사합니다. (옵션은 고급 모드에서만 사용 가능)

압축파일 검사

이 옵션을 사용하면 압축파일 목록에서 선택한 압축파일을 검사합니다. 이 옵션은 기본 설정으로 선택됩니다.

모든 압축파일 형식

이 옵션을 사용하면 압축파일 목록의 모든 압축파일 형식을 선택하여 검사합니다.

스마트 확장명

이 옵션을 사용하면 **Scanner**에서 파일 확장명이 일반적인 확장명과 다르더라도 파일이 압축된 파일 형식(압축파일)인지 여부를 확인하여 압축파일을 검사합니다. 하지만 이 경우 모든 파일을 열어야 하므로 검사 속도가 느려집니다. 예: *.zip 압축파일에 *.xyz라는 파일 확장명이 지정된 경우 **Scanner**에서는 이 압축파일의 압축을 풀어서 검사합니다. 이 옵션은 기본 설정으로 선택됩니다.

참고

이러한 압축파일 형식만 지원되며 압축파일 목록에 표시됩니다.

재귀 수준 제한

재귀적 압축파일의 압축을 풀어서 검사하려면 컴퓨터 시간과 리소스가 많이 필요할 수 있습니다. 이 옵션을 사용하면 여러 번 압축된 압축파일의 검사 수준을 특정 압축 수준 수(최대 재귀 수준)로 제한할 수 있습니다. 따라서 시간과 컴퓨터 리소스가 절약됩니다.

참고

압축파일에서 바이러스나 사용자 동의 없이 설치된 프로그램을 찾으려면 **Scanner**에서 바이러스나 사용자 동의 없이 설치된 프로그램이 있는 재귀 수준까지 검사해야 합니다.

최대 재귀 수준

최대 재귀 수준을 입력하려면 **재귀 수준 제한** 옵션을 선택해야 합니다. 원하는 재귀 수준을 직접 입력하거나 입력 항목에 있는 오른쪽 화살표 키를 사용할 수 있습니다. 허용되는 값은 1 ~ 99입니다. 표준 값 20을 그대로 사용하는 것이 좋습니다.

기본값

이 버튼은 압축파일 검사에 대해 미리 정의된 값을 복원합니다.

압축파일

이 표시 영역에서는 **Scanner**에서 검사해야 할 압축파일을 설정할 수 있습니다. 이 경우 관련 항목을 선택해야 합니다.

예외

Scanner 검사 시 생략할 파일 개체(고급 모드에만 제공되는 옵션)

이 창의 목록에는 바이러스나 사용자 동의 없이 설치된 프로그램 검사 시 **Scanner**에서 포함하면 안 되는 특정 파일 및 경로가 포함되어 있습니다.

여기에는 어떤 이유로든 일반 검사에 포함하면 안 되는 파일 등과 같이 반드시 필요한 예외 항목만 입력하십시오. 이 목록에 포함되기 전에 이러한 파일에 대해 바이러스나 사용자 동의 없이 설치된 프로그램의 포함 여부를 항상 검사하는 것이 좋습니다.

참고

목록의 항목은 총 6,000자를 초과할 수 없습니다.

경고

이러한 파일은 검사에 포함되지 않습니다!

참고

이 목록에 포함된 파일은 [보고서 파일](#)에 기록됩니다. 여기서 파일을 제외한 이유가 더 이상 존재하지 않을 수도 있으므로 가끔씩 보고서 파일에서 검사되지 않는 파일을 확인하십시오. 이 경우 이 목록에서 해당 파일의 이름을 다시 제거해야 합니다.

입력란

이 입력란에는 수동 검사에 포함되지 않는 파일 개체의 이름을 입력할 수 있습니다. 기본적으로 파일 개체가 입력되어 있지 않습니다.



이 버튼을 사용하여 표시되는 창에서 필요한 파일이나 필요한 경로를 선택할 수 있습니다.

전체 경로와 함께 파일 이름을 입력한 경우 이 파일에 대해서만 감염 여부가 검사되지 않습니다. 경로 없이 파일 이름만 입력하면 경로나 드라이브와 상관없이 이 이름을 사용하는 모든 파일이 검사되지 않습니다.

추가

이 버튼을 사용하면 입력란에 입력한 파일 개체를 표시 창에 추가할 수 있습니다.

삭제

이 버튼은 목록에서 선택한 항목을 삭제합니다. 항목을 선택하지 않으면 이 버튼이 비활성화됩니다.

추론

이 구성 섹션에서는 검색 엔진의 추론에 대한 설정을 설명합니다. (옵션은 고급 모드에서만 사용 가능)

Avira 제품에는 손상 요소에 대응할 특수한 바이러스 서명을 생성하고 바이러스 방지 업데이트가 전달되기 전에 알 수 없는 맬웨어를 사전에 확인할 수 있는 강력한 추론 기능이 포함되어 있습니다. 바이러스를 검색하려면 감염된 코드를 광범위하게 분석하고 조사하여 맬웨어의 특징적인 기능을 찾아야 합니다. 검사 대상 코드가 이러한 특징을 나타내는 경우 해당 코드가 의심스러운 코드로 보고됩니다. 의심스러운 코드가 반드시 실제 맬웨어의 코드를 의미하지는 않습니다. 때로는 오진 문제가 발생할 수도 있습니다. 감염된 코드를 처리하는 방법은 코드의 출처를 신뢰할 수 있는지 여부에 따라 사용자가 결정해야 합니다.

매크로 바이러스 추론

매크로 바이러스 추론

Avira 제품에는 강력한 매크로 바이러스 추론이 포함되어 있습니다. 이 옵션을 사용하면 관련 문서의 모든 매크로가 복구 시 삭제되거나 의심스러운 문서만 보고됩니다. 즉 사용자에게 경고가 표시됩니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

AHeAD(고급 추론 분석 및 검색)

AHeAD 사용

Avira 제품에는 AntiVir AheAD 기술 형태의 매우 강력한 추론 기능을 제공하므로 알 수 없는 새로운 맬웨어를 검색할 수 있습니다. 이 옵션을 활성화하면 이 추론의 공격성 수준을 정의할 수 있습니다. 이 옵션은 기본 설정으로 선택됩니다.

낮은 검색 수준

이 옵션을 사용하면 에서 알 수 없는 맬웨어가 검색되는 일이 매우 적으므로 오진 문제가 발생할 위험이 매우 낮습니다.

보통 검색 수준

이 옵션은 오진 문제 발생 위험이 적으면서 강력한 검색 수준을 제공합니다. 이 추론을 사용하도록 선택한 경우 이 설정이 기본 설정이 됩니다.

높은 검색 수준

이 옵션을 사용하면 알 수 없는 더 많은 맬웨어가 검색되지만 가양상 문제가 발생할 가능성이 높습니다.

12.1.2 보고서

Scanner에서는 포괄적인 보고 기능을 제공합니다. 따라서 수동 검사 결과에 대한 정확한 정보를 얻을 수 있습니다. 보고서 파일에는 시스템의 모든 항목은 물론 수동 검사에 대한 알림과 메시지도 포함됩니다. (옵션은 고급 모드에서만 사용 가능)

참고

바이러스나 사용자 동의없이 설치된 프로그램이 발견될 때 Scanner에서 수행되는 작업을 설정하려면 고급 모드 구성에서 보고서 파일을 활성화해야 합니다.

보고

해제

이 옵션을 사용하면 Scanner에서 수동 검사에 대한 작업 및 결과를 보고하지 않습니다.

기본값

이 옵션을 활성화하면 **Scanner**에서 관련 파일의 이름과 경로를 기록합니다. 또한 현재 검사에 구성, 버전 정보 및 라이선스 보유자에 대한 정보도 보고서 파일에 기록됩니다.

확장

이 옵션을 활성화하면 **Scanner**에서 기본 정보와 함께 알림 및 팁을 기록합니다. 이 보고서에는 **Protection Cloud**에서 발견된 항목을 식별하기 위한 '(cloud)' 접미사도 포함되어 있습니다.

완료

이 옵션이 활성화된 경우 **Scanner**에서 검사한 모든 파일을 기록합니다. 또한 알림 및 팁은 물론 관련된 모든 파일이 보고서 파일에 포함됩니다.

참고

문제 해결을 위해 지원 센터로 보고서 파일을 보내야 하는 경우 이 모드에서 이 보고서 파일을 만드십시오.

12.2 Real-Time Protection

구성의 **Real-Time Protection** 섹션에서는 액세스 검사를 구성할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

12.2.1 검사

일반적으로는 시스템을 지속적으로 모니터링하게 됩니다. **Real-Time Protection(= 실시간 Scanner)**은 이 용도로 사용됩니다. 그러면 컴퓨터에 열려 있거나 복사되는 모든 파일을 대상으로 바이러스와 사용자 동의 없이 설치된 프로그램을 즉시 검사할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

파일

Real-Time Protection에서는 필터를 사용하여 특정 확장명(형식)이 지정된 파일만 검사할 수 있습니다.

모든 파일

이 옵션을 선택하면 파일 콘텐츠와 파일 확장명에 관계없이 모든 파일을 대상으로 바이러스와 사용자 동의 없이 설치된 프로그램을 검사합니다.

참고

모든 파일을 사용하는 경우 **파일 확장명** 버튼을 선택할 수 없습니다.

스마트 확장명 사용

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 있는지 검사할 파일이 자동으로 선택됩니다. 즉, 이 프로그램에서 파일 콘텐츠에 따라 파일을 검사할지 여부를 결정합니다. 이 절차는 **파일 확장명 목록 사용**보다는 다소 느리지만 파일 확장명만을 기준으로 검사하지 않으므로 더 정확합니다.

참고

스마트 확장명 사용을 사용하면 **파일 확장명** 버튼을 선택할 수 없습니다.

파일 확장명 목록 사용

이 옵션을 사용하면 지정된 확장명의 파일만 검사합니다. 바이러스와 사용자 동의 없이 설치된 프로그램을 포함할 수 있는 모든 파일 형식이 미리 설정되어 있습니다. "**파일 확장명**" 버튼을 통해 목록을 수동으로 편집할 수 있습니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

참고

이 옵션을 사용하고 파일 확장명 목록에서 모든 항목을 삭제한 경우 **파일 확장명** 버튼 아래에 "파일 확장명 없음"이라는 텍스트가 표시됩니다.

파일 확장명

이 버튼을 사용하면 대화 상자 창이 열리고 이 창에 "**파일 확장명 목록 사용**" 모드에서 검사될 모든 파일 확장명이 표시됩니다. 확장명에 대한 기본 항목이 설정되어 있지만 항목을 추가하거나 삭제할 수 있습니다.

참고

파일 확장명 목록은 버전마다 다를 수 있습니다.

검사 모드

여기에는 파일의 검사 시간이 정의됩니다.

읽을 때 검사

이 옵션을 사용하면 파일을 응용 프로그램 또는 운영 체제에서 읽거나 실행하기 전에 **Real-Time Protection**에서 먼저 검사합니다.

쓸 때 검사

이 옵션을 사용하면 **Real-Time Protection**에서 파일에 쓸 때 파일을 검사합니다. 이 프로세스를 완료한 후에만 파일에 다시 액세스할 수 있습니다.

읽거나 쓸 때 검사

이 옵션을 사용하면 파일을 열거나 읽거나 실행하기 전에, 그리고 파일에 쓰기 전에 **Real-Time Protection**에서 파일을 검사합니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

드라이브

네트워크 드라이브 모니터링

이 옵션을 사용하면 서버 볼륨, 피어 드라이브 등 네트워크 드라이브(매핑된 드라이브)의 파일을 검사합니다.

참고

컴퓨터의 성능이 크게 저하되지 않도록 하려면 **네트워크 드라이브 모니터링**은 예외적인 경우에만 사용해야 합니다.

경고

이 옵션을 사용하지 않으면 네트워크 드라이브가 모니터링되지 **않습니다**. 따라서 바이러스나 사용자 동의 없이 설치된 프로그램으로부터 더 이상 보호되지 않습니다.

참고

네트워크 드라이브에서 파일을 실행하는 경우 **네트워크 드라이브 모니터링** 옵션에 대한 설정과 관계없이 **Real-Time Protection**에서 해당 파일을 검사합니다. 경우에 따라 **네트워크 드라이브 모니터링** 옵션이 사용되지 않더라도 네트워크 드라이브의 파일을 여는 동안 파일이 검사될 수도 있습니다. 이유: 이러한 파일이 '파일 실행' 권한으로 액세스되기 때문입니다. 이러한 파일이나 네트워크 드라이브에서 실행된 파일을 **Real-Time Protection**의 검사 대상에서 제외하려면 제외할 파일 개체 목록에 파일을 입력합니다([Real-Time Protection > 검사 > 예외 참조](#)).

캐싱 사용

이 옵션을 사용하면 네트워크 드라이브에서 모니터링된 파일을 **Real-Time Protection**의 캐시에서 사용할 수 있습니다. 캐시 기능을 사용하지 않고 네트워크 드라이브를 모니터링하는 것이 보다 안전하지만 캐시를 사용할 경우에 비해 모니터링이 제대로 수행되지 않습니다.

압축

압축 파일 검사

이 옵션을 사용하면 압축 파일을 검사합니다. 압축된 파일을 검사하고 나서 압축이 풀린 파일을 다시 검사합니다. 이 옵션은 기본적으로 비활성화됩니다. 압축 파일 검사는 재귀 수준, 검사할 파일 수 및 압축 파일 크기를 사용하여 제한할 수 있습니다. 최대 재귀 수준, 검사할 파일 수 및 최대 압축 파일 크기를 설정할 수 있습니다.

참고

이 옵션은 컴퓨터 처리 성능이 많이 요구되므로 기본적으로 비활성화됩니다. 일반적으로 압축 파일은 수동 검사를 사용하여 검사하는 것이 좋습니다.

최대 재귀 수준

압축 파일을 검사할 때 **Real-Time Protection**에서는 재귀 검사를 사용합니다. 즉, 압축 파일 안에 들어 있는 압축 파일도 압축을 풀어서 바이러스나 사용자 동의 여부와 관계 없이 설치된 프로그램이 있는지 검사합니다. 재귀 수준을 사용자가 정의할 수 있습니다. 권장 재귀 수준은 1로, 기본 압축 파일 자체에 위치한 모든 파일을 검사합니다.

최대 파일 수

압축 파일을 검사할 때 압축 파일에서 최대 파일 수를 지정하여 검사를 제한할 수 있습니다. 검사할 최대 파일 수에 대한 기본값은 10이며 이 값을 그대로 사용하는 것이 좋습니다.

최대 크기(KB)

압축 파일을 검사할 때 압축을 풀 최대 압축 파일의 크기를 지정하여 검사를 제한할 수 있습니다. 표준 값인 1,000KB를 사용하는 것이 좋습니다.

검색 시 작업

바이러스나 사용자 동의 없이 설치된 프로그램을 발견했을 때 **Real-Time Protection**에서 수행할 작업을 정의할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

대화형

이 옵션을 선택하면, **Real-Time Protection**이 바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견했을 때 데스크톱 알림이 나타납니다. "**세부 정보**" 버튼을 통해, 발견된 맬웨어를 제거하거나 다른 바이러스 처리 작업에 액세스할 수 있습니다. 작업이 대화 상자에 표시됩니다. 이 옵션은 기본 설정으로 선택됩니다.

허용되는 작업

이 표시란에서는 대화 상자에서 추가 작업으로 사용할 바이러스 관리 작업을 지정할 수 있습니다. 이를 위해서는 해당 옵션을 활성화해야 합니다.

복구

가능한 경우 **Real-Time Protection** 기능이 감염된 파일을 복구합니다.

이름 바꾸기

Real-Time Protection에서 파일 이름을 바꿉니다. 따라서 더블클릭과 같은 방법으로 이러한 파일에 더 이상 직접 액세스할 수 없습니다. 나중에 파일을 복구한 후 이름을 원래 상태로 되돌릴 수 있습니다.

격리 저장소

검사 프로그램에서 파일을 격리 저장소로 옮깁니다. 해당 파일이 정보가 포함된 중요한 파일인 경우 격리 관리자를 통해 복구하거나 필요한 경우 **Avira** 맬웨어 연구 센터로 보낼 수 있습니다. 파일에 따라 격리 관리자에서 추가 선택 옵션을 사용할 수 있습니다.

삭제

파일이 삭제됩니다. 이 프로세스는 **덮어쓰기 및 삭제**보다 훨씬 빠릅니다(아래 참조).

무시

파일에 대한 액세스가 허용되고 파일을 무시합니다.

덮어쓰기 및 삭제

Real-Time Protection에서 파일을 삭제하기 전에 파일을 기본 패턴으로 덮어씁니다. 이 파일은 복원할 수 없습니다.

경고

Real-Time Protection이 **Scan when writing**으로 설정되는 경우 영향받는 파일은 작성되지 않습니다.

기본값

이 버튼을 사용하면 바이러스가 발견될 때 대화 상자에서 활성화되는 작업을 선택할 수 있습니다. 기본적으로 활성화할 작업을 선택하고 "**기본값**" 버튼을 클릭합니다.

참고

복구 작업은 기본 작업으로 선택할 수 없습니다.

자세한 내용을 보려면 [여기를 클릭하십시오](#).

자동

이 옵션을 사용하면 바이러스가 검색되어도 대화 상자가 표시되지 않습니다. **Real-Time Protection**에서는 이 섹션에서 기본 및 보조 작업으로 미리 정의하는 설정에 따라 작동합니다.

작업 전에 격리 저장소로 복사

이 옵션을 사용하면 **Real-Time Protection**에서 요청한 기본 작업 또는 보조 작업을 수행하기 전에 백업 복사본을 만듭니다. 백업 복사본은 격리 저장소에 저장됩니다. 파일에 정보 값이 있는 경우 격리 관리자를 통해 파일을 복원할 수 있습니다. 또한 추가 조사를 위해 백업 복사본을 **Avira** 맬웨어 연구 센터로 보낼 수 있습니다. 개체에 따라 격리 관리자에서 추가 선택 옵션을 사용할 수 있습니다.

기본 작업

기본 작업은 **Real-Time Protection**에서 바이러스나 사용자 동의 없이 설치된 프로그램을 찾을 때 수행하는 작업입니다. "복구" 옵션을 선택했지만 영향받는 파일을 복구할 수 없는 경우 "보조 작업"에 선택된 작업이 수행됩니다.

참고

기본 작업 아래에서 **복구** 설정을 선택한 경우에만 **보조 작업** 옵션을 선택할 수 있습니다.

복구

이 옵션을 사용하면 **Real-Time Protection**에서 영향받는 파일을 자동으로 복구합니다. 영향받는 파일을 복구할 수 없는 경우 **Real-Time Protection**에서는 **보조 작업**에 선택된 작업을 수행합니다.

참고

자동 복구를 사용하는 것이 좋지만, 이 경우 **Real-Time Protection**에서 워크스테이션의 파일을 수정하게 됩니다.

이름 바꾸기

이 옵션이 사용하도록 설정된 경우 **Real-Time Protection**에서 파일 이름을 바꿉니다. 따라서 더블클릭과 같은 방법으로 이러한 파일에 더 이상 직접 액세스할 수 없습니다. 파일을 나중에 복구하고 원래 이름을 다시 지정할 수 있습니다.

격리 저장소

이 옵션을 사용하면 **Real-Time Protection**에서 파일을 격리 저장소로 이동합니다. 이 디렉터리의 파일은 나중에 복구하거나 필요할 경우 **Avira** 맬웨어 연구 센터로 보낼 수 있습니다.

삭제

이 옵션을 사용하면 파일이 삭제됩니다. 이 프로세스는 **덮어쓰기 및 삭제**보다 훨씬 빠릅니다.

무시

이 옵션을 사용하면 파일에 액세스할 수 있고 파일이 그대로 유지됩니다.

경고

영향받는 파일은 워크스테이션에서 활성 상태로 유지됩니다. 이로 인해 워크스테이션에 심각한 손상이 발생할 수 있습니다.

덮어쓰기 및 삭제

이 옵션을 사용하는 경우 **Real-Time Protection**이 파일을 기본 패턴으로 덮어쓴 다음 삭제합니다. 이 파일은 복원할 수 없습니다.

액세스 거부

보고서 기능이 활성화되어 있는 경우 이 옵션을 사용하면 **Real-Time Protection**에서 **보고서 파일**에 검색 정보만 입력합니다. 또한 이 옵션을 사용하면 **이벤트 로그**에 항목을 씁니다.

경고

Real-Time Protection이 **쓸 때 검사**로 설정된 경우 영향받는 파일이 작성되지 않습니다.

보조 작업

기본 작업 아래에서 **복구** 옵션을 선택한 경우에만 **보조 작업**을 선택할 수 있습니다. 이 옵션을 사용하면 영향받는 파일을 복구할 수 없는 경우 해당 파일에 대해 수행할 작업을 결정할 수 있습니다.

이름 바꾸기

이 옵션이 사용하도록 설정된 경우 **Real-Time Protection**에서 파일 이름을 바꿉니다. 따라서 더블클릭과 같은 방법으로 이러한 파일에 더 이상 직접 액세스할 수 없습니다. 파일을 나중에 복구하고 원래 이름을 다시 지정할 수 있습니다.

격리 저장소

이 옵션을 사용하면 **Real-Time Protection**에서 파일을 격리 저장소로 이동합니다. 이러한 파일은 나중에 복구하거나 필요할 경우 **Avira** 맬웨어 연구 센터로 보낼 수 있습니다.

삭제

이 옵션을 사용하면 파일이 삭제됩니다. 이 프로세스는 **덮어쓰기 및 삭제**보다 훨씬 빠릅니다.

무시

이 옵션을 사용하면 파일에 액세스할 수 있고 파일이 그대로 유지됩니다.

경고

영향받는 파일은 워크스테이션에서 활성 상태로 유지됩니다. 이로 인해 워크스테이션에 심각한 손상이 발생할 수 있습니다.

덮어쓰기 및 삭제

이 옵션을 사용하는 경우 **Real-Time Protection**이 파일을 기본 패턴으로 덮어쓴 다음 삭제합니다. 이 파일은 복원할 수 없습니다.

액세스 거부

보고서 기능이 활성화되어 있는 경우 이 옵션을 사용하면 **Real-Time Protection**에서 [보고서 파일](#)에 검색 정보만 입력합니다. 또한 이 옵션을 사용하면 [이벤트 로그](#)에 항목을 씁니다.

참고

삭제나 덮어쓰기 및 삭제를 기본 또는 보조 작업으로 선택한 경우 추론(heuristic)이 적용하는 경우 영향받는 파일이 삭제되지 않고 격리 저장소 보관소로 이동됩니다.

추가 작업

이벤트 로그 사용

이 옵션을 사용하면 발견될 때마다 항목이 이벤트 로그에 추가됩니다. **Windows** 이벤트 뷰어에서 이벤트를 불러올 수 있습니다. 이 옵션은 기본 설정으로 선택됩니다. (옵션은 고급 모드에서만 사용 가능)

예외

이러한 옵션을 사용하면 **Real-Time Protection**(실시간 검사)에 대한 예외 개체를 구성할 수 있습니다. 그러면 해당 개체가 실시간 검사에 포함되지 않습니다. **Real-Time Protection**에서는 생략할 프로세스의 목록을 통해 실시간 검사 중에 이러한 개체에 대한 파일 액세스를 무시할 수 있습니다. 이 기능은 데이터베이스 또는 백업 솔루션을 사용하는 경우 등에 유용합니다. (옵션은 고급 모드에서만 사용 가능)

생략할 프로세스 및 파일 개체를 지정할 때 다음 사항에 유의하십시오. 목록은 맨 위에서부터 아래로 내려가며 처리됩니다. 목록이 길수록 프로세서에서 각 액세스에 대해 목록을 처리하는 데 걸리는 시간이 길어집니다. 따라서 목록을 가능한 짧게 유지하십시오.

*Real-Time Protection*을 통해 생략될 프로세스

이 목록에 있는 프로세스에 대한 모든 파일 액세스가 **Real-Time Protection**을 통한 모니터링에서 제외됩니다.

입력란

이 항목에 실시간 검사에서 무시할 프로세스의 이름을 입력합니다. 기본적으로 프로세스 이름이 입력되어 있지 않습니다.

프로세스의 경로 및 파일 이름은 **255**자 이내로 지정해야 합니다. 최대 **128**개의 프로세스를 입력할 수 있습니다. 목록의 항목은 총 **6,000**자를 초과할 수 없습니다.

프로세스를 입력할 때 유니코드 기호가 허용됩니다. 따라서 특수 기호를 포함하는 프로세스나 디렉터리 이름을 입력할 수 있습니다.

드라이브 정보는 [드라이브 문자]:\ 형태로 입력해야 합니다.

콜론 기호(:)는 드라이브를 지정하는 데만 사용됩니다.

프로세스를 지정할 때 와일드카드 *(임의 개수 문자)와 ? (단일 문자)를 사용할 수 있습니다.

```
C:\Program Files\Application\application.exe
C:\Program Files\Application\applicatio?.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\*.exe
```

프로세스가 **Real-Time Protection**에서 전체적으로 제외되지 않도록 하기 위해 *(별표), ? (물음표), /(슬래시), \ (역슬래시), .(마침표), :(콜론) 문자로만 구성된 지정은 유효하지 않습니다.

전체 경로 세부 정보가 없어도 **Real-Time Protection**에서 프로세스가 모니터링되지 않도록 할 수 있습니다. 예: application.exe

하지만 이 작동은 실행 파일이 하드 디스크 드라이브에 있는 프로세스에만 적용됩니다.

실행 파일이 연결된 드라이브(예: 네트워크 드라이브)에 있는 프로세스에는 전체 경로 세부 정보가 필요합니다. [연결된 네트워크 드라이브에 대한 예외 표기에 대한 일반 정보를 참조하십시오.](#)

실행 파일이 동적 드라이브에 있는 프로세스에는 예외를 지정하지 마십시오. 동적 드라이브는 **CD**, **DVD** 또는 **USB** 스틱 같은 이동식 디스크에 사용됩니다.

경고

목록에 기록된 프로세스에 의한 모든 파일 액세스가 바이러스 및 사용자 동의 없이 설치된 프로그램 검사에서 제외됩니다.



이 버튼을 누르면 실행 파일을 선택할 수 있는 창이 열립니다.

프로세스

"프로세스" 버튼을 누르면 실행 중인 프로세스가 표시되는 "프로세스 선택" 창이 열립니다.

추가

이 버튼을 사용하면 입력란에 입력된 프로세스를 표시 창에 추가할 수 있습니다.

삭제

이 버튼을 사용하면 선택한 프로세스를 표시 창에서 삭제할 수 있습니다.

*Real-Time Protection*을 통해 생략될 파일 개체

이 목록에 있는 프로세스에 대한 모든 파일 액세스가 **Real-Time Protection**을 통한 모니터링에서 제외됩니다.

입력란

이 상자에 실시간 검사에 포함되지 않는 파일 개체의 이름을 입력할 수 있습니다. 기본적으로 파일 개체가 입력되어 있지 않습니다.

이 목록의 항목은 총 문자 수가 **6,000**자를 넘지 않아야 합니다.

생략할 파일 개체를 지정하는 경우 와일드카드 *(임의 개수 문자)와 ? (단일 문자)를 사용할 수 있습니다. 개별 파일 확장명을 제외할 수도 있습니다(와일드카드 포함).

```
C:\Directory\*.mdb
```

```
*.mdb
```

```
*.md?
```

```
*.xls*
```

```
C:\Directory\*.log
```

디렉터리 이름은 역슬래시(\)로 끝나야 합니다.

디렉터리가 제외되는 경우 모든 하위 디렉터리도 자동으로 제외됩니다.

각 드라이브에 대해 드라이브 문자로 시작하는 전체 경로를 입력하여 최대 **20**개의 예외를 지정할 수 있습니다. 예:

```
C:\Program Files\Application\Name.log
```

전체 경로가 없는 최대 예외 수는 **64**개입니다. 예:

```
*.log
```

```
\computer1\C\directory1
```

다른 드라이브의 디렉터리로 탑재되는 동적 드라이브의 경우 예외 목록에서 통합 드라이브의 운영 체제 별칭을 사용해야 합니다. 예:

```
\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
```

C:\DynDrive와 같이 탑재 지정 자체를 사용하는 경우에는 동적 드라이브가 검사됩니다. **Real-Time Protection** 보고서 파일에서 사용할 운영 체제의 별칭을 결정할 수 있습니다.



이 버튼은 제외할 파일 개체를 선택할 수 있는 창을 엽니다.

추가

이 버튼을 사용하면 입력란에 입력한 파일 개체를 표시 창에 추가할 수 있습니다.

삭제

이 버튼을 사용하면 선택한 파일 개체를 표시 창에서 삭제할 수 있습니다.

예외를 지정할 때 다음 사항에 유의하십시오.

짧은 DOS 파일 이름(DOS 이름 규칙 8.3)을 사용하여 액세스하는 개체도 제외하려면 해당 짧은 파일 이름도 목록에 입력해야 합니다.

와일드카드를 포함하는 파일 이름은 백슬래시로 끝낼 수 없습니다. 예:

C:\Program Files\Application\application*.exe\

이 항목은 유효하지 않으므로 예외로 간주되지 않습니다!

연결된 네트워크 드라이브에 대한 예외와 관련하여 다음 사항에 유의하십시오. 연결된 네트워크 드라이브의 드라이브 문자를 사용하는 경우 지정된 파일 및 폴더가 **Real-Time Protection** 검사에서 제외됩니다. 예외 목록의 **UNC** 경로가 네트워크 드라이브에 연결하는 데 사용되는 **UNC** 경로와 다른 경우(예외 목록의 IP 주소 지정 - 네트워크 드라이브에 연결하기 위한 컴퓨터 이름 지정) 지정된 폴더와 파일이 **Real-Time Protection** 검사에서 제외되지 않습니다. **Real-Time Protection** 보고서 파일에서 관련 **UNC** 경로를 찾으십시오. \\<컴퓨터 이름>\<Enable>\ - 또는- \\<IP 주소>\<Enable>\

Real-Time Protection 보고서 파일에서 감염된 파일을 검사하는 데 사용하는 경로를 찾을 수 있습니다. 예외 목록에 동일한 경로를 지정하십시오. 다음과 같이 진행하십시오. **Real-Time Protection > 보고서** 아래 구성에서 **Real-Time Protection**의 프로토콜 기능을 **완료**로 설정합니다. 이제 **Real-Time Protection**을 활성화한 상태에서 파일, 폴더, 탑재된 드라이브 또는 연결된 네트워크 드라이브에 액세스합니다. 이제 **Real-Time Protection** 보고서 파일에서 사용될 경로를 읽을 수 있습니다. 보고서 파일은 제어 센터의 로컬 보호 > **Real-Time Protection**에서 액세스할 수 있습니다.

추론

이 구성 섹션에서는 검색 엔진의 추론에 대한 설정을 설명합니다. (옵션은 고급 모드에서만 사용 가능)

Avira 제품에는 손상 요소에 대응할 특수한 바이러스 서명을 생성하고 바이러스 방지 업데이트가 전달되기 전에 알 수 없는 맬웨어를 사전에 확인할 수 있는 강력한 추론 기능이 포함되어 있습니다. 바이러스를 검색하려면 감염된 코드를 광범위하게 분석하고 조사하여 맬웨어의 특징적인 기능을 찾아야 합니다. 검사 대상 코드가 이러한 특징을 나타내는 경우 해당 코드가 의심스러운 코드로 보고됩니다. 의심스러운 코드가 반드시 실제 맬웨어의

코드를 의미하지는 않습니다. 때로는 오진 문제가 발생할 수도 있습니다. 감염된 코드를 처리하는 방법은 코드의 출처를 신뢰할 수 있는지 여부에 따라 사용자가 결정해야 합니다.

매크로 바이러스 추론

매크로 바이러스 추론

Avira 제품에는 강력한 매크로 바이러스 추론이 포함되어 있습니다. 이 옵션을 사용하면 관련 문서의 모든 매크로가 복구 시 삭제되거나 의심스러운 문서만 보고됩니다. 즉 사용자에게 경고가 표시됩니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

AHeAD(고급 추론 분석 및 검색)

AHeAD 사용

Avira 제품에는 AntiVir AHeAD 기술 형태의 매우 강력한 추론 기능을 제공하므로 알 수 없는 새로운 맬웨어를 검색할 수 있습니다. 이 옵션을 활성화하면 이 추론의 공격성 수준을 정의할 수 있습니다. 이 옵션은 기본 설정으로 선택됩니다.

낮은 검색 수준

이 옵션을 사용하면 알 수 없는 맬웨어가 검색되는 일이 매우 적으므로 오진 문제가 발생할 위험이 매우 낮습니다.

보통 검색 수준

이 옵션은 오진 문제 발생 위험이 적으면서 강력한 검색 수준을 제공합니다. 이 추론을 사용하도록 선택한 경우 이 설정이 기본 설정이 됩니다.

높은 검색 수준

이 옵션을 사용하면 알 수 없는 더 많은 맬웨어가 검색되지만 가양상 문제가 발생할 가능성이 높습니다.

12.2.2 보고서

Real-Time Protection에는 사용자 또는 관리자에게 검색 유형 및 방식에 대한 정확한 정보를 제공하기 위한 광범위한 로깅 기능이 포함됩니다. (옵션은 고급 모드에서만 사용 가능.)

보고

이 그룹에서는 보고서 파일의 콘텐츠를 결정할 수 있습니다.

해제

이 옵션을 사용하면 **Real-Time Protection**에서 로그를 만들지 않습니다. 평가판을 실행하여 여러 바이러스나 사용자 동의 없이 설치된 프로그램을

테스트하려는 경우처럼 예외적인 상황이 아니면 로깅 기능을 해제하지 않는 것이 좋습니다.

기본값

이 옵션을 사용하면 **Real-Time Protection**에서 바이러스 발견, 알람 및 오류 관련 중요 정보를 보고서 파일에 기록하고 중요 항목의 보다 확실한 전달을 위해 중요도가 낮은 정보는 무시합니다. 이 옵션은 기본 설정으로 선택됩니다.

확장

이 옵션을 사용하면 **Real-Time Protection**에서 덜 중요한 정보도 보고서 파일에 기록합니다.

완료

이 옵션을 사용하면 **Real-Time Protection**에서 파일 크기, 파일 형식, 날짜 등 사용할 수 있는 모든 정보를 보고서 파일에 기록합니다.

보고서 파일 제한

nMB로 크기 제한

이 옵션을 사용하면 보고서 파일을 특정 크기로 제한할 수 있습니다. 허용되는 값은 1~100MB입니다. 보고서 파일의 크기를 제한하여 시스템 리소스 사용을 최소화하면 약 50KB의 추가 공간이 확보됩니다. 로그 파일의 크기가 지정된 크기를 50KB 이상 초과하는 경우에는 지정된 크기 - 50KB의 크기가 될 때까지 오래된 항목이 삭제됩니다.

줄이기 전에 보고서 파일 백업

이 옵션을 사용하면 보고서 파일의 크기를 줄이기 전에 보고서 파일을 백업합니다.

보고서 파일에 구성 쓰기

이 옵션을 사용하면 실시간 검사의 구성이 보고서 파일에 기록됩니다.

참고

보고서 파일 제한을 지정하지 않은 경우 보고서 파일이 100MB에 도달하면 새 보고서 파일이 자동으로 생성됩니다. 이전 보고서 파일의 백업이 생성됩니다. 이전 보고서 파일에 대해 최대 세 개 백업이 저장됩니다. 가장 오래된 백업부터 삭제됩니다.

12.3 업데이트

업데이트 섹션에서는 업데이트 자동 받기 . 여러 가지 업데이트 간격을 지정하고

자동 업데이트

모든 n일/시간/분

이 상자에서는 자동 업데이트가 수행되는 간격을 지정할 수 있습니다. 업데이트 간격을 변경하려면 상자에서 시간 옵션 중 하나를 강조 표시하고 입력 상자의 오른쪽에 있는 화살표 키를 사용하여 변경합니다.

인터넷에 연결(전화 접속)하는 동안 작업 시작

이 옵션을 선택하면 지정된 업데이트 간격 이외에 인터넷에 연결될 때마다 업데이트 작업이 수행됩니다. (옵션은 고급 모드에서만 사용 가능)

시간이 만료된 경우 작업 반복

이 옵션을 선택하면 컴퓨터 전원이 꺼지는 등의 이유로 인해 지정된 시간에 수행할 수 없었던 지난 업데이트 작업이 수행됩니다(옵션은 고급 모드에서만 사용 가능).

12.3.1 웹 서버

웹 서버

인터넷의 웹 서버를 통해 업데이트를 직접 수행할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

웹 서버 연결

기존 연결(네트워크) 사용

이 설정은 네트워크를 통해 연결되는 경우에 표시됩니다.

다음 연결 사용

이 설정은 연결을 개별적으로 정의하는 경우에 표시됩니다.

업데이트 프로그램에서 사용할 수 있는 연결 옵션을 자동으로 검색합니다. 사용할 수 없는 연결 옵션은 회색으로 표시되고 활성화할 수 없습니다. 예를 들면 Windows의 전화 번호부 항목을 통해 전화 접속 연결을 수동으로 설정할 수 있습니다

사용자

선택한 계정의 사용자 이름을 입력합니다.

암호

이 계정에 대한 암호를 입력합니다. 보안을 유지하기 위해 이 공간에 입력하는 실제 문자는 별표(*)로 대체됩니다.

참고

기존 인터넷 계정 이름이나 암호를 잊은 경우 인터넷 서비스 공급자에게 문의하십시오.

참고

전화 접속 도구(예: SmartSurfer, Oleco 등)를 통한 업데이트 프로그램의 자동 전화 접속은 아직 사용할 수 없습니다.

업데이트를 위해 설정된 전화 접속 연결 종료

이 옵션을 사용하면 다운로드가 성공적으로 완료되면 즉시 업데이트를 위해 설정된 전화 접속 연결이 자동으로 중단됩니다.

참고

이 옵션은 Windows XP에서만 사용할 수 있습니다. 이후 운영 체제에서는 업데이트를 위해 열린 전화 접속 연결이 다운로드 수행 즉시 종료됩니다.

프록시 설정*프록시 서버***프록시 서버 사용 안 함**

이 옵션을 선택하면 웹 서버에 연결할 때 프록시 서버가 사용되지 않습니다.

프록시 시스템 설정 사용

이 옵션을 선택하면 프록시 서버를 통해 웹 서버에 연결할 때 현재 Windows 시스템 설정이 사용됩니다. 제어판 > 인터넷 옵션 > 연결 > LAN 설정에서 프록시 서버를 사용하도록 Windows 시스템 설정을 구성합니다. Internet Explorer의 추가 기능 메뉴에서 인터넷 옵션에 액세스할 수도 있습니다.

경고

인증이 필요한 프록시 서버를 사용하는 경우 이 프록시 서버 사용 옵션에서 필요한 데이터를 모두 입력하십시오. 프록시 시스템 설정 사용 옵션은 인증이 없는 프록시 서버에만 사용할 수 있습니다.

이 프록시 서버 사용

웹 서버 연결이 프록시 서버를 통해 설정되는 경우 여기에 관련 정보를 입력할 수 있습니다.

주소

웹 서버에 연결할 때 사용할 프록시 서버의 컴퓨터 이름 또는 IP 주소를 입력합니다.

포트

웹 서버에 연결할 때 사용할 프록시 서버의 포트 번호를 입력합니다.

로그인 이름

프록시 서버에 로그인할 사용자 이름을 입력합니다.

로그인 암호

프록시 서버에 로그인하기 위한 해당 암호를 입력합니다. 보안을 유지하기 위해 이 공간에 입력하는 실제 문자는 별표(*)로 대체됩니다.

예:

주소: proxy.domain.com 포트: 8080

주소: 192.168.1.100 포트: 3128

12.4 Backup

구성 > 로컬 보호 > **Backup**에서 Avira Backup 기능을 구성할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

12.4.1 설정

설정에서는 백업 구성 요소의 동작을 구성할 수 있습니다.

수정한 파일만 백업

이 옵션을 사용하면 증분형 백업(마지막 백업이 백업 프로필에 저장된 이후에 수정된 파일)이 생성됩니다. 이 옵션을 사용하지 않도록 설정하면 각각의 저장된 백업 프로필마다 전체 백업이 생성됩니다(백업 프로필에 모든 파일이 저장됨). 이 옵션은 기본적으로 사용하도록 설정되며 증분 백업이 전체 데이터 백업 백업보다 속도도 빠르고 리소스도 덜 사용되므로 이 옵션을 사용하는 것이 좋습니다.

백업 이전에 바이러스 및 사용자 동의 없이 설치된 프로그램 검사

이 옵션을 사용하면 백업 중에 저장되는 파일의 바이러스 및 맬웨어를 검사합니다. 감염된 파일은 저장되지 않습니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

12.4.2 예외

예외에서는 백업 작업 시 저장할 파일 개체 및 형식과, 저장하지 않을 파일 개체 및 형식을 지정할 수 있습니다.

백업에서 건너뛴 파일

이 창의 이 목록에는 백업에 저장되지 않은 파일과 경로가 들어 있습니다.

참고

목록의 항목은 총 6000자를 초과할 수 없습니다.

참고

이 목록에 포함된 파일은 [보고서 파일](#)에 기록됩니다.

입력란

저장하지 않을 파일 개체의 이름을 이 상자에 입력합니다. 로그인한 사용자의 로컬 설정에 대한 임시 디렉터리 경로가 기본값으로 입력됩니다.



이 버튼을 사용하여 표시되는 창에서 필요한 파일이나 필요한 경로를 선택할 수 있습니다.

파일의 전체 이름 및 경로를 사용하여 백업에서 특정 파일을 제외할 수 있습니다. 파일 이름이나 경로를 입력하면 경로나 드라이브와 상관없이 이 이름을 사용하는 모든 파일이 저장되지 않습니다.

추가

이 버튼을 사용하면 입력란에 입력한 파일 개체를 표시 창에 추가할 수 있습니다.

삭제

이 버튼은 목록에서 선택한 항목을 삭제합니다. 항목을 선택하지 않으면 이 버튼이 비활성화됩니다.

목록 다시 설정

이 버튼은 미리 정의된 기본값을 복원합니다.

다음 사항에 주의하십시오.

- 파일 이름에는 와일드카드 *(임의 개수의 문자)와 ? (단일 문자)만 포함될 수 있습니다.
- 목록은 맨 위에서부터 아래 순서로 처리됩니다.
- 디렉터리가 제외되는 경우 모든 하위 디렉터리도 자동으로 제외됩니다.
- 개별 파일 확장명을 제외할 수도 있습니다(와일드카드 포함).
- 짧은 DOS 파일 이름(DOS 이름 규칙 8.3)을 사용하여 액세스하는 개체도 제외하려면 해당 짧은 파일 이름도 목록에 입력해야 합니다.

참고

와일드카드를 포함하는 파일 이름은 백슬래시로 끝낼 수 없습니다. 예:
C:\Program Files\Application\application*.exe\
이 항목은 유효하지 않으므로 예외로 간주되지 않습니다!

예:

- application.exe
- \Program Files\
C:*.*
- C:*
- *.exe
- *.xl?
- *.*
- C:\Program Files\Application\application.exe
- C:\Program Files\Application\application*.exe
- C:\Program Files\Application\application*
- C:\Program Files\Application\application?????.e*
- C:\Program Files\
C:\Program Files
- C:\Program Files\Application*.mdb

파일 확장명 목록**모든 파일 확장명 고려**

이 옵션을 사용하면 백업 프로파일의 모든 파일이 저장됩니다.

제외할 파일 확장명 목록 사용

이 옵션을 사용하면 백업 프로파일의 모든 파일이 저장되지만 제외된 파일 확장명 목록에 확장명이 입력되어 있는 파일은 제외됩니다.

파일 확장명

이 버튼은 "제외할 파일 확장명 목록 사용" 옵션을 사용하도록 설정한 경우 백업 시 저장되지 않는 모든 파일 확장명을 표시하는 대화 상자를 엽니다. 확장명에 대한 기본 항목이 설정되어 있지만 항목을 추가하거나 삭제할 수 있습니다.

포함할 파일 확장명 목록 사용

이 옵션을 사용하면 고려할 파일 확장명 목록에 파일 확장명이 입력된 파일만 저장됩니다.

파일 확장명

이 버튼은 "포함할 파일 확장명 목록 사용" 옵션을 사용하도록 설정한 경우 백업 시 저장된 모든 파일 확장명을 표시하는 대화 상자를 엽니다. 확장명에 대한 기본 항목이 설정되어 있지만 항목을 추가하거나 삭제할 수 있습니다.

12.4.3 보고서

백업 구성 요소에는 광범위한 로그 기능이 포함되어 있습니다.

보고

이 그룹에서는 보고서 파일의 콘텐츠를 결정할 수 있습니다.

해제

이 옵션을 선택하면 백업 구성 요소가 로그를 생성하지 않습니다. 로깅 기능은 특별한 경우가 아니면 해제하지 마십시오.

기본값

이 옵션을 사용하면 백업 구성 요소에서 저장, 바이러스 발견, 알림 및 오류에 대한 중요 정보를 보고서 파일에 기록하며, 중요 항목을 보다 확실하게 전달하기 위해 중요도가 낮은 정보는 무시합니다. 이 옵션은 기본 설정으로 선택됩니다.

확장

이 옵션을 선택하면 백업 구성 요소는 중요도가 낮은 정보도 보고서 파일에 포함합니다.

완료

이 옵션을 선택하면 백업 구성 요소는 백업 프로세스 및 바이러스 검사에 대한 모든 정보를 보고서 파일에 포함합니다.

12.5 FireWall

12.5.1 FireWall 구성

Avira Internet Security에서는 Avira FireWall을 구성하거나.

- [Avira FireWall](#)

12.5.2 Avira FireWall

구성 > **Internet Protection** 아래의 **FireWall** 섹션에서는 Avira FireWall을 구성합니다.

어댑터 규칙

Avira FireWall에서 어댑터는 소프트웨어 시뮬레이트된 하드웨어 장치(예: 미니포트, 브리지 연결 등) 또는 실제 하드웨어 장치(예: 네트워크 카드)를 나타냅니다.

Avira FireWall에서는 컴퓨터에서 드라이버가 설치된 기존의 모든 어댑터에 대한 어댑터 규칙을 표시합니다. (옵션은 고급 모드에서만 사용 가능)

- ICMP 프로토콜
- TCP 포트 검사
- UDP 포트 검사
- 들어오는 규칙
- 나가는 규칙
- 규칙을 관리하는 버튼

미리 정의된 어댑터 규칙은 보안 수준에 따라 다릅니다. 제어 센터의 **인터넷 보호 > FireWall**에서 *보안* 수준을 변경하거나 사용자 고유의 어댑터 규칙을 정의할 수 있습니다. 제어 센터의 **FireWall** 섹션에서 사용자 고유의 어댑터 규칙을 정의한 경우 *보안* 수준이 사용자 지정으로 설정됩니다.

참고

Avira FireWall의 미리 정의된 모든 규칙에 대한 기본 *보안* 수준 설정은 높음입니다.

ICMP 프로토콜

Internet Control Message Protocol(ICMP)는 네트워크에서 오류 및 정보 메시지를 교환하는 데 사용됩니다. 이 프로토콜은 ping 또는 tracer를 이용한 상태 메시지에도 사용됩니다. 이 규칙을 사용하면 들어오고 나가는 메시지 중 차단되는 메시지 유형, 플로딩 동작 및 조각화된 ICMP 패킷의 반응을 정의할 수 있습니다. 이 규칙은 모든 패킷에 응답하므로 공격을 받은 컴퓨터의 CPU 로드를 증가시키는 ICMP 플로드 공격을 방지하는 역할을 수행합니다.

ICMP 프로토콜에 대해 미리 정의된 규칙

설정	규칙
낮음	수신 차단된 유형: 유형 없음. 발신 차단된 유형: 유형 없음. 패킷 간 지연이 50밀리초보다 짧으면 플로딩으로 간주합니다. 조각화된 ICMP 패킷을 거부합니다.
보통	낮은 수준에도 동일한 규칙이 적용됩니다.
높음	수신 차단된 유형: 여러 유형 발신 차단된 유형: 여러 유형 패킷 간 지연이 50밀리초보다 짧으면 플로딩으로 간주합니다. 조각화된 ICMP 패킷을 거부합니다.

수신 차단된 유형: 유형 없음/여러 유형

이 링크를 클릭하면 ICMP 패킷 유형 목록이 표시됩니다. 이 목록에서 차단할 수신 ICMP 메시지 유형을 지정할 수 있습니다.

발신 차단된 유형: 유형 없음/여러 유형

이 링크를 클릭하면 ICMP 패킷 유형 목록이 표시됩니다. 이 목록에서 차단할 발신 ICMP 메시지 유형을 선택할 수 있습니다.

플로딩으로 간주

이 링크를 클릭하면 허용되는 최대 ICMPPA 지연을 입력할 수 있는 대화 상자가 나타납니다. 예: 50밀리초.

조각화된 ICMP 패킷

이 링크를 클릭하면 조각화된 ICMP 패킷의 "거부 및 거부 안함" 여부를 선택할 수 있습니다.

TCP 포트 검사

이 규칙을 사용하면 Firewall에서 TCP 포트 검사로 간주하는 경우와 이 경우에 수행해야 할 작업을 정의할 수 있습니다. 이 규칙은 컴퓨터에 열려 있는 TCP 포트를 감지하는 TCP 포트 검사 공격을 방지하는 역할을 수행합니다. 이러한 종류의 공격은 컴퓨터에서 취약점을 검색하는 데 사용되며 보다 위험한 공격 유형으로 이어지는 경우가 많습니다.

TCP 포트 검사에 대해 미리 정의된 규칙

설정	규칙
낮음	50개 이상의 포트가 5,000 밀리초 안에 검사된 경우 TCP 포트 검사로 간주합니다. 발견되면 공격자의 IP를 기록하고 공격을 차단하는 규칙을 추가하지 않습니다.
보통	50개 이상의 포트가 5,000 밀리초 안에 검사된 경우 TCP 포트 검사로 간주합니다. 발견되면 공격자의 IP를 기록하고 공격을 차단하는 규칙을 추가합니다.
높음	중간 수준에도 동일한 규칙이 적용됩니다.

포트

이 링크를 클릭하면 몇 개의 포트가 검사될 경우 TCP 포트 검사로 간주할지를 입력할 수 있는 대화 상자가 나타납니다.

포트 검사 시간 창

이 링크를 클릭하면 TCP 포트 검사로 간주할 특정 포트 검사 횟수에 대한 시간 범위를 입력할 수 있는 대화 상자가 나타납니다.

이벤트 데이터베이스

이 링크를 클릭하면 공격자의 IP 주소에 대한 "기록 및 기록 안 함" 여부를 선택할 수 있습니다.

규칙

이 링크를 클릭하면 TCP 포트 검사 공격을 차단하는 규칙의 "추가 및 추가 안 함" 여부를 선택할 수 있습니다.

UDP 포트 검사

이 규칙을 사용하면 FireWall에서 UDP 포트 검사로 간주하는 경우와 이 경우에 수행해야 할 작업을 정의할 수 있습니다. 이 규칙은 컴퓨터에 열려 있는 UDP 포트를 감지하는 UDP 포트 검사 공격을 방지합니다. 이러한 종류의 공격은 컴퓨터에서 취약점을 검색하는 데 사용되며 보다 위험한 공격 유형으로 이어지는 경우가 많습니다.

UDP 포트 검사에 대해 미리 정의된 규칙

설정	규칙
낮음	50개 이상의 포트가 5,000 밀리초 안에 검사될 경우 UDP 포트 검사로 간주합니다. 발견되면 공격자의 IP를 기록하고 공격을 차단하는 규칙을 추가하지 않습니다.
보통	50개 이상의 포트가 5,000 밀리초 안에 검사될 경우 UDP 포트 검사로 간주합니다. 발견되면 공격자의 IP를 기록하고 공격을 차단하는 규칙을 추가합니다.
높음	중간 수준에도 동일한 규칙이 적용됩니다.

포트

이 링크를 클릭하면 몇 개의 포트가 검사될 경우 UDP 포트 검사로 간주할지를 입력할 수 있는 대화 상자가 나타납니다.

포트 검사 시간 창

이 링크를 클릭하면 UDP 포트 검사로 간주할 특정 포트 검사 횟수에 소요되는 시간을 입력할 수 있는 대화 상자가 나타납니다.

이벤트 데이터베이스

이 링크를 클릭하면 공격자의 IP 주소에 대한 "기록 및 기록 안 함" 여부를 선택할 수 있습니다.

규칙

이 링크를 클릭하면 TCP 포트 검사 공격을 차단하는 규칙의 "추가 및 추가 안 함" 여부를 선택할 수 있습니다.

들어오는 규칙

들어오는 규칙은 Avira FireWall에서 들어오는 트래픽을 제어하기 위해 정의됩니다.

경고

패킷이 필터링될 경우 해당 규칙이 차례차례 적용되므로 규칙 순서가 매우 중요합니다. 수행하는 작업에 대해 잘 알고 있는 경우에만 규칙 순서를 변경하십시오.

TCP 트래픽 모니터에 대해 미리 정의된 규칙

설정	규칙
낮음	들어오는 트래픽을 Avira FireWall에서 차단하지 않습니다.
보통	<p>135에서 설정된 TCP 연결 허용 로컬 포트가 {135}이고 원격 포트가 {0-65535}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 TCP 패킷을 허용합니다. 기존 연결 패킷에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 오프셋 0에서 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.</p> <p>135에서 TCP 패킷 거부 로컬 포트가 {135}이고 원격 포트가 {0-65535}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 TCP 패킷을 거부합니다. 모든 패킷에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 오프셋 0에서 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.</p> <p>TCP 정상 트래픽 모니터 로컬 포트가 {0-65535}이고 원격 포트가 {0-65535}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 TCP 패킷을 허용합니다. 연결 시작 및 기존 연결 패킷에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 오프셋 0에서 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.</p> <p>TCP 패킷 거부 로컬 포트가 {0-65535}이고 원격 포트가 {0-65535}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 TCP 패킷을 거부합니다. 모든 패킷에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 오프셋 0에서 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.</p>

높음	<p>설정된 TCP 트래픽 모니터 로컬 포트가 {0-65535}이고 원격 포트가 {0-65535}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 TCP 패킷을 허용합니다.</p> <p>기존 연결 패킷에 적용됩니다.</p> <p>패킷이 규칙과 일치하는 경우 기록하지 않습니다.</p> <p>고급: 오프셋 0에서 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.</p>
----	---

TCP 패킷 허용/거부

이 링크를 클릭하면 특별하게 정의된 들어오는 TCP 패킷을 허용할지 거부할지 여부를 선택할 수 있습니다.

IP 주소

이 링크를 클릭하면 필요한 IPv4/IPv6 주소를 입력할 수 있는 대화 상자가 열립니다.

IP 마스크

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

로컬 포트

이 링크를 클릭하면 로컬 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

원격 포트

이 링크를 클릭하면 원격 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

적용 방법

이 링크를 클릭하면 "모든 패킷"이 아닌 "기존 연결 패킷"에 대해서만 규칙을 적용하거나 "연결 시작 및 기존 연결 패킷"에 대해 규칙을 적용할 수 있습니다.

이벤트 데이터베이스

이 링크를 클릭하면 패킷이 규칙을 준수하는 경우 이벤트 데이터베이스에 "기록 및 기록 안 함" 여부를 결정할 수 있습니다.

고급

고급 기능을 사용하면 콘텐츠를 필터링할 수 있습니다. 예를 들어 특정 오프셋에 특정 데이터를 포함하는 패킷을 거부할 수 있습니다. 이 옵션을 사용하지 않으려면 파일을 선택하지 않거나 빈 파일을 선택하십시오.

필터링된 콘텐츠: 바이트

이 링크를 클릭하면 특정 버퍼를 포함하는 파일을 선택할 수 있는 대화 상자가 나타납니다.

필터링된 콘텐츠: 마스크

이 링크를 클릭하면 특정 마스크를 선택할 수 있는 대화 상자가 나타납니다.

필터링된 콘텐츠: 오프셋

이 링크를 클릭하면 필터링된 콘텐츠 오프셋을 정의할 수 있는 대화 상자가 나타납니다. 오프셋은 TCP 헤더가 끝나는 위치부터 계산됩니다.

UDP 트래픽 모니터에 대해 미리 정의된 규칙

설정	규칙
낮음	-
보통	<p>UDP 허용 트래픽 모니터 로컬 포트가 {0-65535}이고 원격 포트가 {0-65535}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 UDP 패킷을 허용합니다. 모든 스트림에 대한 열린 포트에 규칙을 적용합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 오프셋 0에서 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.</p> <p>UDP 패킷 무시 로컬 포트가 {0-65535}이고 원격 포트가 {0-65535}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 UDP 패킷을 거부합니다. 모든 스트림에 대한 열린 포트에 규칙을 적용합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 오프셋 0에서 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.</p>

높음	<p>설정된 UDP 트래픽 모니터 로컬 포트가 {0-65535}이고 원격 포트가 {53, 67, 68, 123}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 UDP 패킷을 허용합니다. 모든 스트림에 대해 열린 포트에 규칙을 적용합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 오프셋 0에서 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.</p>
----	---

UDP 패킷 허용/거부

이 링크를 클릭하면 특별하게 정의된 들어오는 UDP 패킷을 허용할지 거부할지 여부를 선택할 수 있습니다.

IP 주소

이 링크를 클릭하면 필요한 IPv4/IPv6 주소를 입력할 수 있는 대화 상자가 열립니다.

IP 마스크

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

로컬 포트

이 링크를 클릭하면 로컬 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

원격 포트

이 링크를 클릭하면 원격 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

적용 방법

포트

이 링크를 클릭하면 규칙을 모든 포트에 적용할지 아니면 열려 있는 모든 포트에만 적용할지 선택할 수 있습니다.

스트림

이 링크를 클릭하면 이 규칙을 모든 스트림에 적용할지 아니면 아웃바운드 스트림에만 적용할지 선택할 수 있습니다.

이벤트 데이터베이스

이 링크를 클릭하면 패킷이 규칙을 준수하는 경우 이벤트 데이터베이스에 "기록 및 기록 안 함" 여부를 결정할 수 있습니다.

고급

고급 기능을 사용하면 콘텐츠를 필터링할 수 있습니다. 예를 들어 특정 오프셋에 특정 데이터를 포함하는 패킷을 거부할 수 있습니다. 이 옵션을 사용하지 않으려면 파일을 선택하지 않거나 빈 파일을 선택하십시오.

필터링된 콘텐츠: 바이트

이 링크를 클릭하면 특정 버퍼를 포함하는 파일을 선택할 수 있는 대화 상자가 나타납니다.

필터링된 콘텐츠: 마스크

이 링크를 클릭하면 특정 마스크를 선택할 수 있는 대화 상자가 나타납니다.

필터링된 콘텐츠: 오프셋

이 링크를 클릭하면 필터링된 콘텐츠 오프셋을 정의할 수 있는 대화 상자가 나타납니다. 오프셋은 **UDP** 헤더가 끝나는 위치부터 계산됩니다.

ICMP 트래픽 모니터에 대해 미리 정의된 규칙

설정	규칙
낮음	-
보통	<p>IP 주소를 기반으로 ICMP 무시 안 함 마스크가 0.0.0.0인 주소 0.0.0.0의 ICMP 패킷을 허용합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 오프셋 0에서 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.</p>
높음	중간 수준에도 동일한 규칙이 적용됩니다.

ICMP 패킷 허용/거부

이 링크를 클릭하면 특별하게 정의된 들어오는 **ICMP** 패킷을 허용할지 거부할지 여부를 선택할 수 있습니다.

IP 주소

이 링크를 클릭하면 필요한 **IP** 주소를 입력할 수 있는 대화 상자가 열립니다.

IP 마스크

이 링크를 클릭하면 필요한 **IPv4** 마스크를 입력할 수 있는 대화 상자가 열립니다.

이벤트 데이터베이스

이 링크를 클릭하면 패킷이 규칙을 준수하는 경우 이벤트 데이터베이스에 "**기록 및 기록 안 함**" 여부를 결정할 수 있습니다.

고급

고급 기능을 사용하면 콘텐츠를 필터링할 수 있습니다. 예를 들어 특정 오프셋에 특정 데이터를 포함하는 패킷을 거부할 수 있습니다. 이 옵션을 사용하지 않으려면 파일을 선택하지 않거나 빈 파일을 선택하십시오.

필터링된 콘텐츠: 바이트

이 링크를 클릭하면 특정 버퍼를 포함하는 파일을 선택할 수 있는 대화 상자가 나타납니다.

필터링된 콘텐츠: 마스크

이 링크를 클릭하면 특정 마스크를 선택할 수 있는 대화 상자가 나타납니다.

필터링된 콘텐츠: 오프셋

이 링크를 클릭하면 필터링된 콘텐츠 오프셋을 정의할 수 있는 대화 상자가 나타납니다. 오프셋은 **ICMP** 헤더가 끝나는 위치부터 계산됩니다.

IP 패킷에 대해 미리 정의된 규칙

설정	규칙
낮음	-
보통	-
높음	모든 IP 패킷 거부 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 IPv4 패킷을 거부합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다.

허용/거부

이 링크를 클릭하면 특별히 정의된 **IP** 패키지를 허용할지 거부할지 여부를 결정할 수 있습니다.

IPv4/IPv6

이 링크를 클릭하면 **IPv4** 또는 **IPv6**을 선택할 수 있습니다.

IP 주소

이 링크를 클릭하면 필요한 IPv4/IPv6 주소를 입력할 수 있는 대화 상자가 열립니다.

IP 마스크

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

이벤트 데이터베이스

이 링크를 클릭하면 패킷이 규칙을 준수하는 경우 이벤트 데이터베이스에 기록할지 여부를 결정할 수 있습니다.

나가는 규칙

나가는 규칙은 Avira FireWall에서 나가는 트래픽을 제어하기 위해 정의됩니다. IP, ICMP, UDP 및 TCP 프로토콜 중 하나에 대한 나가는 규칙을 정의할 수 있습니다. [새 규칙 추가](#)를 참조하십시오.

경고

패킷이 필터링될 경우 해당 규칙이 차례차례 적용되므로 규칙 순서가 매우 중요합니다. 수행하는 작업에 대해 잘 알고 있는 경우에만 규칙 순서를 변경하십시오.

규칙을 관리하는 버튼

버튼	설명
규칙 추가	새 규칙을 만들 수 있습니다. 이 버튼을 누르면 새 규칙 추가 대화 상자가 열립니다. 이 대화 상자에서 새 규칙을 선택할 수 있습니다.
규칙 제거	선택한 규칙을 제거합니다.
규칙 위로	선택한 규칙을 한 줄 위로 이동하여 규칙 우선 순위를 높입니다.
규칙 아래로	선택한 규칙을 한 줄 아래로 이동하여 규칙 우선 순위를 낮춥니다.

<p>규칙 이름 바꾸기</p>	<p>선택한 규칙에 다른 이름을 지정할 수 있습니다.</p>
-------------------------	-----------------------------------

참고
 컴퓨터에 있는 모든 어댑터 또는 개별 어댑터에 대해 새 규칙을 추가할 수 있습니다. 모든 어댑터에 대해 어댑터 규칙을 추가하려면 표시되는 어댑터 계층 구조에서 **내 컴퓨터**를 선택하고 **규칙 추가** 버튼을 클릭합니다. **새 규칙 추가**를 참조하십시오.

참고
 규칙을 원하는 위치로 끌어놓음으로써 규칙의 위치를 변경할 수도 있습니다.

새 규칙 추가

이 창에서는 들어오고 나가는 새 규칙을 선택할 수 있습니다. 선택한 규칙은 **어댑터 규칙** 창에 기본 정보와 함께 포함되며 이 위치에서 더 자세히 정의할 수 있습니다. 들어오고 나가는 규칙 외에 추가 규칙을 사용할 수도 있습니다.

사용할 수 있는 규칙

피어 투 피어 네트워크 허용

피어 투 피어 연결 허용: 포트 4662의 들어오는 TCP 통신과 포트 4672의 들어오는 UDP 통신

TCP 포트

이 링크를 클릭하면 허용된 TCP 포트를 입력할 수 있는 대화 상자가 나타납니다.

UDP 포트

이 링크를 클릭하면 허용되는 UDP 포트를 입력할 수 있는 대화 상자가 나타납니다.

VMWARE 연결 허용

VMWare 시스템 간 통신 허용

IP 차단

지정된 IP 주소의 모든 트래픽을 차단합니다.

인터넷 프로토콜 버전

이 링크를 클릭하면 IPv4 또는 IPv6 중에서 선택할 수 있습니다.

IP 주소

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자 창이 열립니다.

서브넷 차단

지정된 IP 주소와 서브넷 마스크의 모든 트래픽 차단

인터넷 프로토콜 버전

이 링크를 클릭하면 IPv4 또는 IPv6 중에서 선택할 수 있습니다.

IP 주소

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자 창이 열립니다.

서브넷 마스크

이 링크를 클릭하면 필요한 서브넷 마스크를 입력할 수 있는 대화 상자 창이 열립니다.

IP 허용

지정된 IP 주소의 모든 트래픽 허용

인터넷 프로토콜 버전

이 링크를 클릭하면 IPv4 또는 IPv6 중에서 선택할 수 있습니다.

IP 주소

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자 창이 열립니다.

서브넷 허용

지정된 IP 주소와 서브넷 마스크의 모든 트래픽 허용

인터넷 프로토콜 버전

이 링크를 클릭하면 IPv4 또는 IPv6 중에서 선택할 수 있습니다.

IP 주소

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자 창이 열립니다.

서브넷 마스크

이 링크를 클릭하면 필요한 서브넷 마스크를 입력할 수 있는 대화 상자 창이 열립니다.

웹 서버 허용

포트 80에 있는 웹 서버의 통신 허용: 포트 80의 들어오는 TCP 통신

포트

이 링크를 클릭하면 웹 서버가 사용하는 포트를 입력할 수 있는 대화 상자가 나타납니다.

VPN 연결 허용

지정된 IP의 VPN(Virtual Private Network) 연결 허용: x 포트의 들어오는 UDP 데이터 트래픽, x 포트의 들어오는 TCP 데이터 트래픽, 프로토콜 ESP(50), GRE(47)를 사용하는 들어오는 IP 데이터 트래픽

인터넷 프로토콜 버전

이 링크를 클릭하면 IPv4 또는 IPv6 중에서 선택할 수 있습니다.

IP 주소

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자 창이 열립니다.

원격 데스크톱 연결 허용

포트 3389에서 "원격 데스크톱" 연결(원격 데스크톱 프로토콜) 허용

포트

이 링크를 클릭하면 허용된 원격 데스크톱 연결에 사용할 포트를 입력할 수 있는 대화 상자가 나타납니다.

VNC 연결 허용

포트 5900에서 VNC(가상 네트워크 컴퓨팅) 연결 허용

포트

이 링크를 클릭하면 허용된 원격 데스크톱 연결에 사용할 포트를 입력할 수 있는 대화 상자가 나타납니다.

파일 및 프린터 공유를 허용합니다.

프린터 및 파일 승인에 대한 액세스 허용: 지정된 IP 주소에서 포트 137, 139로 들어오는 TCP 데이터 트래픽 및 포트 445로 들어오는 UDP 데이터 트래픽.

사용 가능한 들어오는 규칙

- 들어오는 IP 규칙
- 들어오는 ICMP 규칙
- 들어오는 UDP 규칙
- 들어오는 TCP 규칙
- 들어오는 IP 프로토콜 규칙

사용 가능한 나가는 규칙

- 나가는 IP 규칙
- 나가는 ICMP 규칙
- 나가는 UDP 규칙

- 나가는 TCP 규칙
- 나가는 IP 프로토콜 규칙

참고

사용 가능한 들어오는 규칙과 나가는 규칙의 구문은 관련 프로토콜의 미리 정의된 규칙의 구문([FireWall > 어댑터 규칙](#)에서 설명)과 동일합니다.

버튼

버튼	설명
확인	강조 표시된 규칙이 새 어댑터 규칙으로 포함됩니다.
취소	새 규칙을 추가하지 않고 창을 닫습니다.

응용 프로그램 규칙

사용자의 응용 프로그램 규칙

이 목록에는 시스템의 모든 사용자가 포함됩니다. 관리자로 로그인한 경우 규칙을 적용할 사용자를 선택할 수 있습니다. 관리 권한을 가진 사용자가 아닌 경우 현재 로그인한 사용자만 볼 수 있습니다.

응용 프로그램

이 표에는 규칙이 정의된 응용 프로그램의 목록이 표시됩니다. 응용 프로그램 목록에는 Avira FireWall이 설치된 이후에 실행되고 규칙을 저장한 각 응용 프로그램에 대한 설정이 포함되어 있습니다.

일반 보기

열	설명
응용 프로그램	응용 프로그램 이름
활성 연결	응용 프로그램이 연 활성 연결 수입니다.

작업	네트워크 사용 유형과 상관 없이 응용 프로그램에서 네트워크를 사용할 때 Avira FireWall에서 자동으로 수행할 작업을 표시합니다. 이 링크를 클릭하면 다른 작업 유형으로 전환할 수 있습니다. 작업 유형에는 요청 , 허용 또는 거부 가 있습니다. 기본 작업은 요청 입니다.
----	---

고급 구성

응용 프로그램의 네트워크 액세스에 개별 규칙이 필요한 경우 어댑터 규칙을 만들 때와 동일한 방식으로 패킷 필터 기반의 응용 프로그램 규칙을 만들 수 있습니다.

- ▶ 응용 프로그램 규칙의 고급 구성으로 변경하려면 먼저 **구성** 창에서 **고급 모드** 옵션을 활성화합니다.
- ▶ 그런 다음 **구성 > 인터넷 보호 > FireWall > 설정**으로 이동하고 **응용 프로그램** 규칙에서 **고급 설정** 옵션을 선택합니다.
- ▶ **적용** 또는 **확인**을 클릭하여 설정을 저장합니다.
 - ↳ **구성 > 인터넷 보호 > FireWall > 응용 프로그램 규칙** 섹션에서는, 응용 프로그램 규칙 목록에 제목이 **필터링**인 추가 열이 표시되며 여기에는 각 응용 프로그램에 대한 **기본** 항목이 나타납니다.

열	설명
응용 프로그램	응용 프로그램 이름
활성 연결	응용 프로그램이 연 활성 연결 수입니다.

<p>작업</p>	<p>네트워크 사용 유형과 상관 없이 응용 프로그램에서 네트워크를 사용할 때 Avira FireWall에서 자동으로 수행할 작업을 표시합니다.</p> <p>필터링 열에서 기본을 선택하면, 링크를 클릭하여 다른 작업 유형을 선택할 수 있습니다. 값은 요청, 허용 또는 거부입니다.</p> <p>필터링 열에서 고급을 선택하면 규칙 작업 유형이 표시됩니다. 규칙 링크를 클릭하면 응용 프로그램에 대한 특정 규칙을 입력할 수 있는 고급 응용 프로그램 규칙 창이 열립니다.</p>
<p>필터링</p>	<p>필터링 유형을 표시합니다. 링크를 클릭하여 다른 필터링 유형을 선택할 수 있습니다.</p> <p>기본: 단순 필터링의 경우, 소프트웨어 응용 프로그램이 수행하는 모든 네트워크 작업에 대해 지정된 작업이 실행됩니다.</p> <p>고급: 이 유형의 필터링을 사용하면 확장 구성에 추가된 규칙이 적용됩니다.</p>

- ▶ 응용 프로그램에 대한 특정 규칙을 만들려면 필터링 아래에서 고급 항목을 선택합니다.
 - ↳ 그러면 작업 열에 규칙 항목이 표시됩니다.
- ▶ 규칙을 클릭하면 특정 응용 프로그램 규칙을 만들 수 있는 창이 열립니다.

고급 구성에 지정된 응용 프로그램 규칙

고급 응용 프로그램 규칙을 사용하면 응용 프로그램에 대해 지정된 데이터 트래픽을 허용 또는 거부하거나 개별 포트에 대한 수동 수신 대기 허용 또는 거부할 수 있습니다. 다음 옵션을 사용할 수 있습니다.

코드 삽입 허용/거부

코드 삽입은 다른 프로세스의 주소 공간에 작업을 실행할 코드를 삽입하여 해당 프로세스에서 DLL(동적 연결 라이브러리)을 강제로 로드하는 기술입니다. 코드 삽입은 특히 맬웨어에서 다른 프로그램 몰래 코드를 실행하는 데 사용됩니다. 이 방법을 사용하면 FireWall보다 먼저 인터넷에 몰래 액세스할 수 있습니다. 기본 모드에서 코드 삽입은 서명된 모든 응용 프로그램에 대해 사용하도록 설정됩니다.

응용 프로그램 포트에 대한 수동적 수신 대기 허용/거부

트래픽 허용/거부

- 들어오거나 나가는 IP 패킷 허용 또는 거부
- 들어오거나 나가는 TCP 패킷 허용 또는 거부
- 들어오거나 나가는 UDP 패킷 허용 또는 거부

각 응용 프로그램에 대한 규칙을 개수에 제한 없이 만들 수 있습니다. 응용 프로그램 규칙은 표시된 순서대로 실행됩니다(자세한 내용은 [고급 응용 프로그램 규칙 참조](#)).

참고
 응용 프로그램 규칙의 필터링을 **고급**에서 **기본**으로 변경할 경우, 고급 구성의 기존 응용 프로그램 규칙은 영구적으로 삭제되는 것이 아니라 비활성화 상태가 됩니다. **고급** 필터링을 다시 선택하면 기존 고급 응용 프로그램 규칙이 다시 활성화되어 **응용 프로그램 규칙** 구성 창에 표시됩니다.

응용 프로그램 정보

이 상자에서는 응용 프로그램 목록 상자에서 선택된 응용 프로그램에 대한 자세한 정보를 볼 수 있습니다.

- **이름** - 응용 프로그램의 이름입니다.
- **경로** - 실행 파일의 전체 경로입니다.

버튼

버튼	설명
응용 프로그램 추가	새 응용 프로그램 규칙을 만들 수 있습니다. 이 버튼을 누르면 대화 상자가 열립니다. 여기에서 새 규칙을 만드는 데 필요한 응용 프로그램을 선택할 수 있습니다.
규칙 제거	선택한 응용 프로그램 규칙을 제거합니다.
세부 정보 표시	"세부 정보 표시" 창에는 응용 프로그램 목록 상자에서 선택한 응용 프로그램의 세부 정보가 표시됩니다(고급 모드에서만 사용 가능한 옵션).
다시 로드	응용 프로그램 목록을 다시 로드하고 변경 내용을 취소합니다.

고급 응용 프로그램 규칙

고급 응용 프로그램 규칙 창에서는 응용 프로그램의 데이터 트래픽 및 포트 수신으로 지정된 규칙을 만들 수 있습니다. **규칙 추가** 버튼을 사용하여 새 규칙을 만들 수 있습니다. 창의 하단에서 규칙을 구체적으로 지정할 수 있습니다. 응용 프로그램에 대한 규칙을 개수에 제한 없이 만들 수 있습니다. 규칙은 표시된 순서대로 실행됩니다. **규칙 위로** 및 **규칙 아래로** 버튼을 사용하여 규칙의 순서를 변경할 수 있습니다.

참고

마우스를 사용하여 응용 프로그램 규칙을 필요한 위치로 끌어서 응용 프로그램 규칙의 위치를 변경할 수 있습니다.

응용 프로그램 정보

선택한 응용 프로그램에 관한 정보가 *응용 프로그램 정보* 영역에 표시됩니다.

- *이름* - 응용 프로그램의 이름입니다.
- *경로* - 응용 프로그램 실행 파일의 경로입니다.

규칙 옵션

코드 삽입 허용/거부

이 링크를 마우스로 클릭하여 선택한 응용 프로그램에 코드 삽입을 허용할지 또는 거부할지를 결정할 수 있습니다.

규칙 유형: 트래픽/수신 대기

이 링크를 마우스로 클릭하여 데이터 모니터링 규칙을 만들지 아니면 포트 수신 대기용 규칙을 만들지를 결정할 수 있습니다.

거부/허용 작업

이 링크를 클릭하여 규칙을 통해 실행할 작업을 결정할 수 있습니다.

포트

이 링크를 클릭하면 "수신 대기" 규칙을 적용할 로컬 포트를 입력할 수 있는 대화 상자가 나타납니다. 여러 포트 또는 포트 영역을 입력할 수도 있습니다.

나가는 트래픽, 들어오는 트래픽, 모든 패키지

이 링크를 클릭하면 트래픽 규칙이 나가는 패킷만 모니터링할지 아니면 들어오는 패킷만 모니터링할지를 결정할 수 있습니다.

IP 패킷/TCP 패킷/UDP 패킷

이 링크를 클릭하여 트래픽 규칙을 모니터링하는 프로토콜을 결정할 수 있습니다.

IP 패키지 옵션:

IP 주소

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

IP 마스크

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

TCP 패키지/UDP 패키지 옵션:

로컬 IP 주소

이 링크를 클릭하면 로컬 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

로컬 IP 마스크

이 링크를 클릭하면 필요한 로컬 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

원격 IP 주소

이 링크를 클릭하면 필요한 원격 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

원격 IP 마스크

이 링크를 클릭하면 필요한 원격 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

로컬 포트

이 링크를 클릭하면 로컬 포트 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 열립니다.

원격 포트

이 링크를 클릭하면 하나 이상의 원격 포트 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

보고서 파일

링크를 클릭하면 규칙 충족 시 프로그램의 보고서 파일에 로그를 기록할지("로그"), 기록하지 않을지("로그 안 함") 선택할 수 있습니다.

버튼

버튼	설명
규칙 추가	새 응용 프로그램 규칙을 만듭니다.
규칙 제거	선택한 응용 프로그램 규칙을 삭제합니다.
규칙 위로	선택한 규칙을 한 줄 위로 이동하여 규칙 우선 순위를 높입니다.
규칙 아래로	선택한 규칙을 한 줄 아래로 이동하여 규칙 우선 순위를 낮춥니다.

규칙 이름 바꾸기	선택한 규칙을 편집하여 새 규칙 이름을 입력할 수 있습니다.
적용	변경 내용을 승인하고 Avira FireWall에 즉시 적용합니다.
확인	변경 내용을 적용합니다. 응용 프로그램 규칙 구성 창이 닫힙니다.
취소	변경 내용을 적용하지 않고 응용 프로그램 규칙 구성 창을 닫습니다.

신뢰할 수 있는 공급업체

신뢰할 수 있는 소프트웨어 제조업체 목록은 **신뢰할 수 있는 공급업체** 아래에 표시됩니다.
(옵션은 고급 모드에서만 사용 가능)

네트워크 이벤트 팝업 창의 이 공급자를 항상 신뢰 옵션을 사용하여 목록에 공급자를 추가하거나 목록에서 공급자를 제거할 수 있습니다. **신뢰할 수 있는 공급업체가 응용 프로그램을 자동으로 허용** 옵션을 사용하여 기본적으로 나열된 공급자가 서명한 응용 프로그램의 네트워크 액세스를 허용할 수 있습니다.

사용자의 신뢰할 수 있는 공급업체

이 목록에는 시스템의 모든 사용자가 포함됩니다. 관리자로 로그인한 경우 신뢰할 수 있는 공급자 목록을 보거나 업데이트하려는 사용자를 선택할 수 있습니다. 관리 권한을 가진 사용자가 아닌 경우 현재 로그인한 사용자만 볼 수 있습니다.

신뢰할 수 있는 공급업체가 만든 응용 프로그램을 자동으로 허용

이 옵션을 사용하면 신뢰할 수 있으며 확인된 공급자의 서명과 함께 제공된 응용 프로그램에 대해 네트워크 액세스가 자동으로 허용됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

공급업체

이 목록에는 신뢰할 수 있는 공급업체로 분류된 공급업체가 모두 표시됩니다.

버튼

버튼	설명
제거	강조 표시된 항목을 신뢰할 수 있는 공급업체 목록에서 제거합니다. 선택한 공급자를 목록에서 영구적으로 제거하려면 구성 창에서 적용 또는 확인 을 클릭합니다.
다시 로드	변경을 취소합니다. 마지막으로 저장된 목록이 로드됩니다.

참고

목록에서 공급업체를 제거한 후 **적용**을 선택하면 해당 공급업체가 목록에서 영구적으로 제거됩니다. **다시 로드**를 사용해도 변경 사항을 취소할 수 없습니다. 하지만 **네트워크 이벤트** 팝업 창의 **이 공급업체를 항상 신뢰** 옵션을 사용하여 공급업체를 신뢰할 수 있는 공급자 목록에 다시 추가할 수 있습니다.

참고

FireWall은 신뢰할 수 있는 공급업체 목록에 항목을 만들기 전에 응용 프로그램 규칙을 우선으로 합니다. 응용 프로그램 규칙을 만들었으며 응용 프로그램 공급업체가 신뢰할 수 있는 공급업체 목록에 나열된 경우 응용 프로그램 규칙이 실행됩니다.

설정

고급 모드에서만 사용할 수 있는 옵션입니다.

고급 옵션

시작 시 **Windows** 방화벽 중지

이 옵션을 사용하면 컴퓨터를 다시 부팅할 때 **Windows Firewall**이 비활성화됩니다. 이 옵션은 기본 설정으로 선택됩니다.

자동 규칙 시간 초과

영구 차단

이 옵션을 사용하면 포트 검사 중에 생성된 규칙 등과 같이 자동으로 생성된 규칙이 유지됩니다.

n초 후 규칙 제거

이 옵션을 사용하면 포트 검사 중에 생성된 규칙 등과 같이 자동으로 생성된 규칙이 사용자가 정의한 시간이 지나면 제거됩니다. 이 옵션은 기본 설정으로 선택됩니다. 이 상자에는 규칙이 제거되기 전에 경과되어야 할 시간(초)을 지정할 수 있습니다.

알림

알림은 방화벽에서 데스크톱 알림을 받을 이벤트를 정의합니다.

포트 검사

이 옵션을 활성화하면 FireWall에서 포트 검사가 발견될 경우 사용자에게 데스크톱 알림이 전달됩니다.

플로딩

이 옵션을 활성화하면 FireWall에서 플로딩 공격이 발견될 경우 사용자에게 데스크톱 알림이 전달됩니다..

차단된 응용 프로그램

이 옵션을 활성화하면 FireWall에서 응용 프로그램의 네트워크 작업을 거부(차단)한 경우 사용자에게 데스크톱 알림이 전달됩니다.

차단된 IP

이 옵션을 활성화하면 방화벽에서 한 IP 주소의 데이터 트래픽을 거부(차단)한 경우 사용자에게 데스크톱 알림이 전달됩니다.

응용 프로그램 규칙

응용 프로그램 규칙 옵션은 [FireWall > 응용 프로그램 규칙](#) 섹션에서 응용 프로그램 규칙에 대한 구성 옵션을 설정하는 데 사용됩니다.

고급 설정

이 옵션을 사용하면 응용 프로그램의 다양한 네트워크 액세스를 개별적으로 조정할 수 있습니다.

기본 설정

이 옵션을 사용하면 응용 프로그램의 다양한 네트워크 액세스에 대해 한 가지 작업만 설정할 수 있습니다.

팝업 설정

고급 모드에서만 사용할 수 있는 옵션입니다.

프로세스 시작 스택 검사

이 옵션을 선택하면, 프로세스 스택 검사를 더 정확하게 제어할 수 있습니다. FireWall은 스택 중 신뢰할 수 없는 프로세스는 하위 프로세스를 통해 네트워크에 액세스할 수 있다고 가정합니다. 따라서 프로세스 스택의 프로세스 중 신뢰할 수 없는 프로세스마다 다른 팝업 창이 표시됩니다. 이 옵션은 기본적으로 사용되지 않습니다.

프로세스당 여러 팝업 허용

이 옵션을 사용하면 응용 프로그램이 네트워크에 연결하려고 할 때마다 팝업이 나타납니다. 또는 첫 번째 연결 시도에 대한 정보만 표시됩니다. 이 옵션은 기본적으로 사용되지 않습니다.

이 응용 프로그램에 대한 작업 기억

항상 사용

이 옵션을 선택하면 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 기본 설정으로 사용하도록 설정됩니다.

항상 사용 안 함

이 옵션을 선택하면 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 기본 설정으로 사용하지 않도록 설정됩니다.

서명된 응용 프로그램에 사용

이 옵션을 선택하면 서명된 응용 프로그램이 네트워크에 액세스할 때 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 자동으로 사용됩니다. 서명된 응용 프로그램은 "신뢰할 수 있는 공급자"를 통해 배포됩니다([신뢰할 수 있는 공급자](#) 참조).

마지막으로 사용된 상태 기억

이 옵션을 사용하면 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 마지막 네트워크 이벤트와 동일한 방식으로 사용됩니다. "이 응용 프로그램에 대한 작업 기억" 옵션이 사용되는 경우 이 옵션은 다음 네트워크 이벤트에 대해 사용됩니다. "이 응용 프로그램에 대한 작업 기억" 옵션이 마지막 네트워크 이벤트에 대해 사용되지 않는 경우 이 옵션은 다음 네트워크 이벤트에 대해서도 사용되지 않습니다.

세부 정보 표시

이 구성 옵션 그룹에서는 **네트워크 이벤트** 창의 세부 정보 표시를 설정할 수 있습니다.

요구 시 세부 정보 표시

이 옵션을 선택하면 요청 시에만 "네트워크 이벤트" 창에 세부 정보가 표시됩니다. 예를 들어 "네트워크 이벤트" 창에서 "세부 정보 표시" 버튼을 클릭하면 세부 정보가 표시됩니다.

항상 세부 정보 표시

이 옵션을 사용하면 "네트워크 이벤트" 창에 세부 정보가 항상 표시됩니다.

마지막으로 사용된 상태 기억

이 옵션을 선택하면 세부 정보 표시가 이전 네트워크 이벤트의 경우와 동일한 방식으로 관리됩니다. 세부 정보가 마지막 네트워크 이벤트 중에 표시되었거나 액세스된 경우 다음 네트워크 이벤트에 대해 세부 정보가 표시됩니다. 세부 정보가 마지막 네트워크 이벤트 중에 숨겨졌거나 표시되지 않은 경우에는 다음 네트워크 이벤트에 대해 세부 정보가 표시되지 않습니다.

12.6 Web Protection

구성 > 인터넷 보호 아래의 **Web Protection** 섹션에서는 Web Protection을 구성할 수 있습니다.

12.6.1 검사

Web Protection은 인터넷에서 웹 브라우저에 로드되는 웹 페이지를 통해 사용자의 컴퓨터로 침투하는 바이러스나 맬웨어를 차단합니다. **검사** 옵션을 사용하여 Web Protection 구성 요소의 동작을 설정할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

검사

IPv6 지원 사용

이 옵션을 선택하면 Web Protection에서 인터넷 프로토콜 버전 6을 지원합니다. 이 옵션은 Windows 8에서의 새로운 또는 변경된 설치에 사용할 수 없습니다.

Drive-by 보호

Drive-by 보호 기능을 사용하면 인라인 프레임이라고 하는 **I-Frame**을 차단하도록 설정할 수 있습니다. **I-Frame**은 HTML 요소로, 웹 페이지의 영역을 구분하는 인터넷 페이지 요소입니다. **I-Frame**을 사용하면 서로 다른 웹 콘텐츠(일반적으로 서로 다른 URL)를 브라우저의 하위 창에서 독립적 문서로 로드하여 표시할 수 있습니다. **I-Frame**은 대부분 배너 광고용으로 사용됩니다. 경우에 따라 **I-Frame**은 맬웨어를 감추는 데 사용되기도 합니다. 이 경우 **I-Frame**의 영역은 브라우저에서 대부분 또는 거의 보이지 않습니다. 의심스러운 **I-Frame** 차단 옵션을 사용하면 **I-Frame**의 로드를 확인하여 차단할 수 있습니다.

의심스러운 I-Frame 차단

이 옵션을 선택하면 사용자가 요청하는 웹 페이지의 I-Frame을 특정 기준에 따라 검사합니다. 요청한 웹 페이지에 의심스러운 I-Frame이 있는 경우 해당 I-Frame이 차단됩니다. I-Frame 창에는 오류 메시지가 표시됩니다.

검색에 대한 작업

바이러스나 사용자 동의 없이 설치된 프로그램을 발견했을 때 Web Protection에서 수행할 작업을 정의할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

대화형

이 옵션을 선택하면 수동 검사 시 바이러스나 사용자 동의 없이 설치된 프로그램이 검색될 때 사용자가 영향받는 파일에 대해 수행할 작업을 선택할 수 있는 대화 상자가 나타납니다. 이 옵션은 기본 설정으로 선택됩니다.

진행률 표시줄 표시

이 옵션을 선택하면 웹 사이트 콘텐츠의 다운로드가 20초 시간 제한을 초과할 경우 다운로드 진행률이 있는 데스크톱 알림이 나타납니다. 이 데스크톱 알림은 데이터 양이 많은 웹 사이트의 다운로드를 위해 설계되었습니다. Web Protection을 사용하여 서핑 중인 경우 웹 사이트 콘텐츠는 인터넷 브라우저에 표시되기 전에 바이러스 및 맬웨어가 검사되므로, 웹 사이트 콘텐츠가 인터넷 브라우저에서 증분식으로 다운로드되지 않습니다. 이 옵션은 기본적으로 사용되지 않습니다.

자세한 내용을 보려면 여기를 클릭하십시오.

자동

이 옵션을 사용하면 바이러스가 검색되어도 대화 상자가 표시되지 않습니다. Web Protection은 사용자가 이 섹션에서 기본 및 보조 작업으로 사전 정의하는 설정에 따라 반응합니다.

기본 작업

기본 작업은 Web Protection이 바이러스 또는 원하지 않는 프로그램을 발견한 경우에 수행되는 작업입니다.

액세스 거부

웹 서버에서 요청한 웹 사이트 및/또는 전송된 모든 데이터나 파일이 사용자의 웹 브라우저로 전송되지 않습니다. 액세스가 거부되었음을 알리는 오류 메시지가 웹 브라우저에 표시됩니다. 보고서 기능이 활성화된 경우 Web Protection에서 보고서 파일에 탐지 정보를 기록합니다.

격리 저장소로 이동

바이러스 또는 맬웨어가 탐지될 경우, 웹 서버에서 요청한 웹 사이트 및/또는 전송된 데이터와 파일이 격리 저장소로 이동됩니다. 영향받는 파일이 중요한 파일인 경우 격리 관리자를 통해 복구하거나 필요한 경우 Avira 맬웨어 연구 센터로 보낼 수 있습니다.

무시

웹 서버에서 요청한 웹 사이트 및/또는 전송된 데이터와 파일을 **Web Protection**이 사용자의 웹 브라우저로 전달합니다. 파일에 대한 액세스가 허용되고 파일을 무시합니다.

경고

영향받는 파일은 워크스테이션에서 활성 상태로 유지됩니다. 이로 인해 워크스테이션에 심각한 손상이 발생할 수 있습니다.

차단된 요청

차단된 요청에서는 **Web Protection**이 차단할 파일 형식과 **MIME** 형식(전송된 데이터의 콘텐츠 형식)을 지정할 수 있습니다. 웹 필터를 사용하면 알려진 피싱 및 맬웨어 **URL**을 차단할 수 있습니다. **Web Protection**은 인터넷에서 사용자 컴퓨터 시스템으로의 데이터 전송을 차단합니다. (옵션은 고급 모드에서만 사용 가능)

*Web Protection*에서 다음 파일 형식/MIME 형식을 차단합니다.

이 목록에 있는 모든 파일 형식 및 **MIME** 형식(전송되는 데이터의 콘텐츠 형식)이 **Web Protection**에 의해 차단됩니다.

입력란

이 입력란에는 **Web Protection**에서 차단할 **MIME** 형식 및 파일 형식의 이름을 입력합니다. 파일 형식의 경우 **.htm**과 같은 파일 확장명을 입력합니다. **MIME** 형식의 경우 미디어 형식과 해당되는 경우 하위 형식을 지정합니다. 두 문을 슬래시로 구분합니다(예: **video/mpeg** 또는 **audio/x-wav**).

참고

Web Protection에 의해 차단되었지만 임시 인터넷 파일로 시스템에 이미 저장되어 있는 파일은 컴퓨터의 인터넷 브라우저를 통해 인터넷에서 로컬로 다운로드할 수 있습니다. 임시 인터넷 파일은 인터넷 브라우저에서 웹 사이트에 더 빨리 액세스할 수 있도록 하기 위해 컴퓨터에 저장되는 파일입니다.

참고

차단된 파일 및 **MIME** 형식 목록은 [Web Protection > 검사 > 예외](#)에서 제외된 파일 및 **MIME** 형식 목록에 입력한 경우 무시됩니다.

참고

파일 형식 및 MIME 형식을 입력할 때는 와일드카드(모든 숫자를 나타내는 * 또는 하나의 문자를 나타내는 ?)를 사용할 수 없습니다.

MIME 형식: 미디어 형식의 예:

- text = 텍스트 파일
- image = 그래픽 파일
- video = 비디오 파일
- audio = 사운드 파일
- application = 특정 프로그램에 연결된 파일

제외된 파일 및 MIME 형식의 예

- application/octet-stream = application/octet-stream MIME 형식 파일(실행 파일 *.bin, *.exe, *.com, *.dll, *.class)은 Web Protection에 의해 차단됩니다.
- application/olescript = application/olescript MIME 형식 파일(ActiveX 스크립트 파일 *.axs)은 Web Protection에 의해 차단됩니다.
- .exe = .exe(실행 파일) 확장명이 붙은 모든 파일이 Web Protection에 의해 차단됩니다.
- .msi = .msi(Windows Installer 파일) 확장명이 붙은 모든 파일이 Web Protection에 의해 차단됩니다.

추가

이 버튼을 사용하면 입력 항목에서 표시 창으로 MIME 및 파일 형식을 복사할 수 있습니다.

삭제

이 버튼은 목록에서 선택한 항목을 삭제합니다. 항목을 선택하지 않으면 이 버튼이 비활성화됩니다.

웹 필터

웹 필터는 내부 데이터베이스를 기반으로 하며 매일 업데이트되고 콘텐츠에 따라 URL을 분류합니다.

웹 필터 활성화

이 옵션을 사용하면 웹 필터 목록에서 선택한 범주와 일치하는 모든 URL이 차단됩니다.

웹 필터 목록

웹 필터 목록에서는 **Web Protection**에서 차단할 **URL**이 포함된 콘텐츠 범주를 선택할 수 있습니다.

참고

Web Protection > 검사 > 예외에서 제외된 **URL** 목록에 포함된 항목의 경우에는 웹 필터가 무시됩니다.

참고

스팸 URL은 스팸 전자 메일로 함께 전송되는 **URL**입니다. **부정/사기** 범주는 웹 페이지에 "가입 만료(**Subscription Expires**)"가 표시되거나 공급자가 비용을 표시하지 않는 서비스를 제공합니다.

예외

이 옵션을 사용하면 **Web Protection** 검사를 위한 **URL**(인터넷 주소)에 대한 파일 형식 및 **MIME** 형식(전송되는 데이터의 콘텐츠 형식)을 기반으로 하는 예외를 설정할 수 있습니다. 지정된 **MIME** 형식 및 **URL**은 **Web Protection**에서 무시됩니다. 즉, 사용자 컴퓨터 시스템으로 전송될 때 바이러스와 맬웨어를 검사하지 않습니다. (옵션은 고급 모드에서만 사용 가능)

*Web Protection*에서 건너뛰는 **MIME** 형식

이 항목에서는 검사 중에 **Web Protection**이 무시할 **MIME** 형식(전송되는 데이터의 콘텐츠 형식)을 선택할 수 있습니다.

*Web Protection*에서 건너뛰는 파일 형식/**MIME** 형식(사용자 정의)

이 목록의 모든 **MIME** 형식(전송되는 데이터의 콘텐츠 형식)은 검사 중 **Web Protection**에서 무시됩니다.

입력란

이 입력란에는 검사 중에 **Web Protection**이 무시할 **MIME** 형식 및 파일 형식의 이름을 입력할 수 있습니다. 파일 형식의 경우 **.htm**과 같은 파일 확장명을 입력합니다. **MIME** 형식의 경우 미디어 형식과 해당되는 경우 하위 형식을 지정합니다. 두 문을 슬래시로 구분합니다(예: **video/mpeg** 또는 **audio/x-wav**).

참고

파일 형식 및 **MIME** 형식을 입력할 때는 와일드카드(모든 숫자를 나타내는 * 또는 하나의 문자를 나타내는 ?)를 사용할 수 없습니다.

경고

제외 목록의 모든 파일 형식 및 콘텐츠 형식이 차단된 요청([Web Protection > 검사 > 차단된 요청](#)에서 차단되는 파일 및 **MIME** 형식의 목록) 또는 **Web Protection**의 추가적인 검사 없이 인터넷 브라우저로 다운로드됩니다. 제외 목록의 모든 항목에 대해 파일 및 **MIME** 형식의 목록에 있는 항목이 차단되고 무시됩니다. 바이러스 및 맬웨어 검사가 수행되지 않습니다.

MIME 형식: 미디어 형식의 예:

- text = 텍스트 파일
- image = 그래픽 파일
- video = 비디오 파일
- audio = 사운드 파일
- application = 특정 프로그램에 연결된 파일

제외된 파일 및 **MIME** 형식의 예:

- audio/ = 모든 오디오 미디어 형식 파일이 **Web Protection** 검사에서 제외됩니다.
- video/quicktime = 모든 **Quicktime** 하위 형식 비디오 파일(*.qt, *.mov)이 **Web Protection** 검사에서 제외됩니다.
- .pdf = 모든 **Adobe PDF** 파일이 **Web Protection** 검사에서 제외됩니다.

추가

이 버튼을 사용하면 입력 항목에서 표시 창으로 **MIME** 및 파일 형식을 복사할 수 있습니다.

삭제

이 버튼은 목록에서 선택한 항목을 삭제합니다. 항목을 선택하지 않으면 이 버튼이 비활성화됩니다.

*Web Protection*에서 건너뛰는 URL

이 목록의 모든 URL은 **Web Protection** 검사에서 제외됩니다.

입력란

이 상자에서는 **Web Protection** 검사에서 제외할 **URL**(인터넷 주소)(예: `www.domainname.com`)을 입력할 수 있습니다. 앞이나 뒤의 점으로 도메인 수준을 표시하여 **URL**의 일부를 지정할 수 있습니다. 예를 들어 도메인의 모든 페이지와 모든 하위 도메인을 지정하려면 `.domainname.com`을 지정합니다. 최상위 도메인(`.com` 또는 `.net`)을 사용하는 모든 웹 사이트를 나타내려면 뒤에 점을 추가합니다(`domainname..`). 앞이나 뒤에 점이 없는 문자열을 지정하면 문자열은 최상위 도메인으로 해석됩니다(예: `net`은 모든 **NET** 도메인 지정(`www.domain.net`)).

참고

URL을 지정할 때 와일드카드 `*`를 사용하여 임의 개수의 문자를 지정할 수 있습니다. 다음과 같이 앞이나 뒤의 점을 와일드카드와 함께 사용하여 도메인 수준을 나타낼 수도 있습니다.

`.domainname.*`

`*.domainname.com`

`.*name*.com`(유효하지만 권장하지는 않음)

`*name*`과 같이 점 없이 지정하면 최상위 수준 도메인의 일부로 해석되므로 권장하지 않습니다.

경고

제외된 **URL** 목록의 모든 웹 사이트가 웹 필터 또는 **Web Protection**의 추가 검사 없이 인터넷 브라우저로 다운로드됩니다. 제외된 **URL** 목록의 모든 항목에 대해 웹 필터의 항목([Web Protection > 검사 > 차단된 요청](#) 참조)이 무시됩니다. 바이러스 및 맬웨어 검사가 수행되지 않습니다. 따라서 신뢰할 수 있는 **URL**은 **Web Protection** 검사에서 제외해야 합니다.

추가

이 버튼을 사용하면 입력 항목에 입력한 **URL**(인터넷 주소)을 뷰어 창으로 복사할 수 있습니다.

삭제

이 버튼은 목록에서 선택한 항목을 삭제합니다. 항목을 선택하지 않으면 이 버튼이 비활성화됩니다.

예: 건너뛰는 URL

- www.avira.com** -또는- **www.avira.com/***
 = 도메인 **www.avira.com**이 포함된 모든 **URL**이 **Web Protection** 검사에서 제외됩니다([www.avira.com/en/pages/index.php](#), [www.avira.com/en/support/index.html](#), [www.avira.com/en/download/index.html](#) 등).

도메인 `www.avira.de`가 포함된 URL은 Web Protection 검사에서 제외되지 않습니다.

- `avira.com -OR- *.avira.com`
= 2차 및 최상위 도메인 `avira.com`이 포함된 모든 URL이 Web Protection 검사에서 제외됩니다. `.avira.com`에 대한 기존의 모든 하위 도메인(`www.avira.com`, `forum.avira.com` 등)에 적용됩니다.
- `avira. -또는- *.avira.*`
= 2차 수준 도메인 `avira`가 있는 모든 URL이 Web Protection 검사에서 제외됩니다. 이는 `.avira`의 모든 기존 최상위 도메인 또는 하위 도메인(`www.avira.com`, `www.avira.de`, `forum.avira.com` 등)에 적용됩니다.
- `.*domain*.*`
문자열 `domain`이 있는 2차 수준 도메인이 포함된 모든 URL(`www.domain.com`, `www.new-domain.de`, `www.sample-domain1.de` 등)이 Web Protection 검사에서 제외됩니다.
- `net -OR- *.net`
= 최상위 수준 도메인 `net`이 포함된 모든 URL(`www.name1.net`, `www.name2.net` 등)이 Web Protection 검사에서 제외됩니다.

경고

Web Protection 검사에서 제외할 URL을 가능한 한 정확하게 입력합니다. 맬웨어 및 사용자 동의 없이 설치된 프로그램을 배포하는 인터넷 페이지가 제외의 전역 지정을 통해 Web Protection 검사에서 제외될 위험이 있으므로 전체 최상위 도메인 또는 2수준 도메인의 일부는 가급적 지정하지 않는 것이 좋습니다. 최소한 전체 2수준 도메인과 최상위 도메인을 지정하는 것이 좋습니다(예: `domainname.com`).

추론

이 구성 섹션에서는 검색 엔진의 추론에 대한 설정을 설명합니다. (옵션은 고급 모드에서만 사용 가능)

Avira 제품에는 손상 요소에 대응할 특수한 바이러스 서명을 생성하고 바이러스 방지 업데이트가 전달되기 전에 알 수 없는 맬웨어를 사전에 확인할 수 있는 강력한 추론 기능이 포함되어 있습니다. 바이러스를 검색하려면 감염된 코드를 광범위하게 분석하고 조사하여 맬웨어의 특징적인 기능을 찾아야 합니다. 검사 대상 코드가 이러한 특징을 나타내는 경우 해당 코드가 의심스러운 코드로 보고됩니다. 의심스러운 코드가 반드시 실제 맬웨어의 코드를 의미하지는 않습니다. 때로는 오진 문제가 발생할 수도 있습니다. 감염된 코드를 처리하는 방법은 코드의 출처를 신뢰할 수 있는지 여부에 따라 사용자가 결정해야 합니다.

매크로 바이러스 추론

Avira 제품에는 강력한 매크로 바이러스 추론이 포함되어 있습니다. 이 옵션을 사용하면 관련 문서의 모든 매크로가 복구 시 삭제되거나 의심스러운 문서만 보고됩니다. 즉

사용자에게 경고가 표시됩니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

AHeAD(고급 추론 분석 및 검색)

AHeAD 사용

Avira 제품에는 AntiVir AHeAD 기술 형태의 매우 강력한 추론 기능을 제공하므로 알 수 없는 새로운 맬웨어를 검색할 수 있습니다. 이 옵션을 활성화하면 이 추론의 공격성 수준을 정의할 수 있습니다. 이 옵션은 기본 설정으로 선택됩니다.

낮은 검색 수준

이 옵션을 사용하면 알 수 없는 맬웨어가 검색되는 일이 매우 적으므로 오진 문제가 발생할 위험이 매우 낮습니다.

보통 검색 수준

이 옵션은 오진 문제 발생 위험이 적으면서 강력한 검색 수준을 제공합니다. 이 추론을 사용하도록 선택한 경우 이 설정이 기본 설정이 됩니다.

높은 검색 수준

이 옵션을 사용하면 알 수 없는 더 많은 맬웨어가 검색되지만 오진 문제가 발생할 가능성이 높습니다.

12.6.2 보고서

Web Protection에는 사용자 또는 관리자에게 탐지 유형 및 방식에 대한 정확한 정보를 제공하기 위한 광범위한 로깅 기능이 있습니다.

보고

이 그룹에서는 보고서 파일의 콘텐츠를 결정할 수 있습니다.

해제

이 옵션을 선택하면 Web Protection은 로그를 만들지 않습니다. 평가판을 실행하여 여러 바이러스나 사용자 동의 없이 설치된 프로그램을 테스트하려는 경우처럼 예외적인 상황이 아니면 로깅 기능을 해제하지 않는 것이 좋습니다.

기본값

이 옵션을 선택하면 Web Protection은 바이러스 발견, 알림 및 오류 관련 중요 정보를 보고서 파일에 기록하고 중요 항목의 보다 확실한 전달을 위해 중요도가 낮은 정보는 무시합니다. 이 옵션은 기본 설정으로 선택됩니다.

고급

이 옵션을 선택하면 **Web Protection**은 덜 중요한 정보도 보고서 파일에 기록합니다.

완료

이 옵션을 선택하면 **Web Protection**은 파일 크기, 파일 형식, 날짜 등 사용할 수 있는 모든 정보를 보고서 파일에 기록합니다.

보고서 파일 제한

nMB로 크기 제한

이 옵션을 사용하면 보고서 파일을 특정 크기로 제한할 수 있습니다. 허용되는 값은 1~100MB입니다. 보고서 파일의 크기를 제한하여 시스템 리소스 사용을 최소화하면 약 50KB의 추가 공간이 확보됩니다. 로그 파일의 크기가 지정된 크기를 50KB 이상 초과하는 경우에는 지정된 크기가 20% 줄어들 때까지 오래된 항목을 삭제합니다.

보고서 파일에 구성 쓰기

이 옵션을 사용하면 실시간 검사의 구성이 보고서 파일에 기록됩니다.

참고

보고서 파일 제한을 지정하지 않은 경우, 보고서 파일이 100MB에 도달하면 오래된 항목이 자동으로 삭제됩니다. 보고서 파일의 크기가 80MB에 도달할 때까지 항목이 삭제됩니다.

12.7 Mail Protection

구성의 **Mail Protection** 섹션에서는 **Mail Protection**을 구성합니다.

12.7.1 검사

Mail Protection을 사용하여 받는 전자 메일에 대해 바이러스 및 맬웨어와 스팸 포함 여부를 검사할 수 있습니다. **Mail Protection**에서는 보내는 전자 메일에 대해 바이러스 및 맬웨어 포함 여부를 검사할 수 있습니다. 보내는 메일이 컴퓨터의 알 수 없는 **봇(bot)**으로부터 전송되는 스팸인 경우 **Mail Protection**에서는 스팸을 보내지 못하도록 보내는 메일을 차단합니다.

받는 전자 메일 검사

이 옵션을 선택하면 받는 전자 메일에서 바이러스 및 맬웨어와 스팸을 검사합니다. **Mail Protection**에서는 **POP3**와 **IMAP** 프로토콜을 지원합니다. 전자 메일 클라이언트에서 전자 메일을 받는 데 사용하는 받은 편지함 계정에 대해 **Mail Protection**에서 모니터링할 수 있도록 설정하십시오.

POP3 계정 모니터링

이 옵션을 사용하면 지정된 포트에서 **POP3** 계정이 모니터링됩니다.

모니터링되는 포트

이 항목에는 **POP3** 프로토콜에서 받은 편지함으로 사용할 포트를 입력해야 합니다. 여러 개의 포트는 쉼표로 구분합니다. (옵션은 고급 모드에서만 사용 가능)

기본값

이 버튼은 지정된 포트를 기본 **POP3** 포트로 재설정합니다. (옵션은 고급 모드에서만 사용 가능)

IMAP 계정 모니터링

이 옵션을 사용하면 지정된 포트에서 **IMAP** 계정이 모니터링됩니다.

모니터링되는 포트

이 항목에는 **IMAP** 프로토콜에서 받은 편지함으로 사용할 포트를 입력해야 합니다. 여러 개의 포트는 쉼표로 구분합니다. (옵션은 고급 모드에서만 사용 가능)

기본값

이 버튼은 지정된 포트를 기본 **IMAP** 포트로 재설정합니다. (옵션은 고급 모드에서만 사용 가능)

보내는 전자 메일 검사(SMTP)

이 옵션을 선택하면 보내는 전자 메일에서 바이러스 및 맬웨어를 검사합니다. 전자 메일이 알 수 없는 보트에서 보내는 스팸일 경우 전자 메일이 차단됩니다.

모니터링되는 포트

이 항목에는 **SMTP** 프로토콜에서 보낸 편지함으로 사용할 포트를 입력해야 합니다. 여러 개의 포트는 쉼표로 구분합니다. (옵션은 고급 모드에서만 사용 가능)

기본값

이 버튼은 지정된 포트를 기본 **SMTP** 포트로 재설정합니다. (옵션은 고급 모드에서만 사용 가능)

참고

사용된 프로토콜 및 포트를 확인하려면 전자 메일 클라이언트 프로그램에서 전자 메일 계정의 속성을 확인하십시오. 대체로 기본 포트가 사용됩니다.

IPv6 지원 사용

이 옵션을 사용하는 경우 **Mail Protection**에서 인터넷 프로토콜 버전 **6**을 지원합니다. (옵션은 고급 모드에서만 사용할 수 있으며, **Windows 8**에서의 새로운 또는 변경된 설치에 사용할 수 없습니다.)

검색에 대한 작업

이 구성 섹션에는 **Mail Protection**에서 전자 메일이나 첨부 파일에서 바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견한 경우 수행하는 작업에 대한 기타 설정이 포함되어 있습니다. (옵션은 고급 모드에서만 사용 가능)

참고

이러한 작업은 받는 전자 메일에서 바이러스가 검색될 때와 보내는 전자 메일에서 바이러스가 검색될 때 모두 수행됩니다.

대화형

이 옵션을 사용하면 전자 메일이나 첨부 파일에서 바이러스나 사용자 동의 없이 설치된 프로그램이 검색될 때 사용자가 관련 파일에 대해 수행할 작업을 선택할 수 있는 대화 상자 창이 나타납니다. 이 옵션은 기본 설정으로 선택됩니다.

진행률 표시줄 표시

이 옵션을 사용하면 **Mail Protection**에서 전자 메일 다운로드 중 진행률 표시줄을 표시합니다. 이 옵션은 "대화형" 옵션을 선택한 경우에만 사용할 수 있습니다.

자동

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 발견된 경우 더 이상 알림이 제공되지 않습니다. 이 섹션에서 정의한 설정에 따라 **Mail Protection**이 작동합니다.

영향받는 전자 메일

"*영향받는 전자 메일*"에 대해 선택한 작업은 **Mail Protection**이 전자 메일에서 바이러스나 사용자 동의 없이 설치된 프로그램을 찾을 때 수행하는 작업입니다. "무시" 옵션을 선택하는 경우 첨부 파일에서 발견된 바이러스나 사용자 동의 없이 설치된 프로그램을 처리하기 위한 프로세스를 "*영향받는 첨부 파일*"에서 선택할 수도 있습니다.

삭제

전자 메일의 본문은 아래 지정된 기본 텍스트로 대체됩니다. 전자 메일의 본문은 아래 지정된 **기본 텍스트**로 대체됩니다. 포함된 모든 첨부 파일에도 동일하게 적용됩니다. 따라서 이러한 첨부 파일도 **기본 텍스트**로 대체됩니다.

무시

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 검색되어도 감염된 전자 메일이 무시됩니다. 하지만 감염된 첨부 파일에 대해 수행할 작업을 결정할 수 있습니다.

격리 저장소로 이동

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 발견된 경우 모든 첨부 파일을 포함한 전체 전자 메일이 격리 저장소에 보관됩니다. 필요할 경우 나중에 복원할 수 있습니다. 감염된 전자 메일 자체는 삭제됩니다. 전자 메일의 본문은 아래 지정된 **기본 텍스트**로 대체됩니다. 포함된 모든 첨부 파일에도 동일하게 적용됩니다. 따라서 이러한 첨부 파일도 **기본 텍스트**로 대체됩니다.

영향받는 첨부 파일

"**영향받는 첨부 파일**" 옵션은 "**영향받는 전자 메일**"에서 "**무시**"를 선택한 경우에만 선택할 수 있습니다. 이 옵션을 사용하면 첨부 파일에서 바이러스나 사용자 동의 없이 설치된 프로그램이 발견될 경우 수행할 작업을 결정할 수 있습니다.

삭제

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 발견된 경우 영향받는 첨부 파일이 삭제되고 **기본 텍스트**로 대체됩니다.

무시

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 검색되어도 첨부 파일이 무시되고 배달됩니다.

경고

이 옵션을 선택하면 **Mail Protection**에서 바이러스나 사용자 동의 없이 설치된 프로그램으로부터 사용자를 보호하지 않습니다. 어떠한 작업을 수행해야 할지 확실히 알고 있는 경우에만 이 항목을 선택하십시오. 전자 메일 프로그램에서 미리 보고를 사용하지 마십시오. 더블클릭해도 첨부 파일이 열리지 않습니다!

격리 저장소로 이동

이 옵션을 사용하면 영향받는 첨부 파일이 격리 저장소로 이동된 다음 삭제됩니다(**기본 텍스트**로 대체됨). 필요할 경우 영향받는 첨부 파일을 나중에 복원할 수도 있습니다.

추가 작업

이 구성 섹션에는 **Mail Protection**에서 전자 메일이나 첨부 파일에서 바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견한 경우 수행하는 작업에 대한 추가 설정이 포함되어 있습니다. (옵션은 고급 모드에서만 사용 가능)

참고

이러한 작업은 받는 전자 메일에서 바이러스가 검색될 때만 수행됩니다.

삭제 및 이동된 전자 메일에 대한 기본 텍스트

이 상자의 텍스트는 영향받는 전자 메일 대신에 전자 메일에 메시지로 삽입됩니다. 이 메시지를 편집할 수 있습니다. 텍스트 길이는 최대 500자입니다.

서식 지정 시 다음 키 조합을 사용할 수 있습니다.

Ctrl + Enter = 줄 바꿈을 삽입합니다.

기본값

이 버튼은 편집 상자에 미리 정의된 기본 텍스트를 삽입합니다.

삭제 및 이동된 첨부 파일에 대한 기본 텍스트

이 상자의 텍스트는 영향받는 첨부 파일 대신에 전자 메일에 메시지로 삽입됩니다. 이 메시지를 편집할 수 있습니다. 텍스트 길이는 최대 500자입니다.

서식 지정 시 다음 키 조합을 사용할 수 있습니다.

Ctrl + Enter = 줄 바꿈을 삽입합니다.

기본값

이 버튼은 편집 상자에 미리 정의된 기본 텍스트를 삽입합니다.

추론

이 구성 섹션에서는 검색 엔진의 추론에 대한 설정을 설명합니다. (옵션은 고급 모드에서만 사용 가능)

Avira 제품에는 손상 요소에 대응할 특수한 바이러스 서명을 생성하고 바이러스 방지 업데이트가 전달되기 전에 알 수 없는 맬웨어를 사전에 확인할 수 있는 강력한 추론 기능이 포함되어 있습니다. 바이러스를 검색하려면 감염된 코드를 광범위하게 분석하고 조사하여 맬웨어의 특징적인 기능을 찾아야 합니다. 검사 대상 코드가 이러한 특징을 나타내는 경우 해당 코드가 의심스러운 코드로 보고됩니다. 의심스러운 코드가 반드시 실제 맬웨어의 코드를 의미하지는 않습니다. 때로는 오진 문제가 발생할 수도 있습니다. 감염된 코드를 처리하는 방법은 코드의 출처를 신뢰할 수 있는지 여부에 따라 사용자가 결정해야 합니다.

매크로 바이러스 추론

Avira 제품에는 강력한 매크로 바이러스 추론이 포함되어 있습니다. 이 옵션을 사용하면 관련 문서의 모든 매크로가 복구 시 삭제되거나 의심스러운 문서만 보고됩니다. 즉 사용자에게 경고가 표시됩니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

AHeAD(고급 추론 분석 및 검색)

AHeAD 사용

Avira 제품에는 AntiVir AHeAD 기술 형태의 매우 강력한 추론 기능을 제공하므로 알 수 없는 새로운 맬웨어를 검색할 수 있습니다. 이 옵션을 활성화하면 이 추론의 공격성 수준을 정의할 수 있습니다. 이 옵션은 기본 설정으로 선택됩니다.

낮은 검색 수준

이 옵션을 사용하면 에서 알 수 없는 맬웨어가 검색되는 일이 매우 적으므로 오진 문제가 발생할 위험이 매우 낮습니다.

보통 검색 수준

이 옵션은 오진 문제 발생 위험이 적으면서 강력한 검색 수준을 제공합니다. 이 추론을 사용하도록 선택한 경우 이 설정이 기본 설정이 됩니다.

높은 검색 수준

이 옵션을 사용하면 알 수 없는 더 많은 맬웨어가 검색되지만 가양상 문제가 발생할 가능성이 높습니다.

AntiBot

Mail Protection의 AntiBot 기능은 사용자의 컴퓨터가 **보트넷**의 일부가 되어 스팸 전자 메일을 전송하는 데 사용되는 것을 방지합니다. 보트넷을 통해 스팸을 보내기 위해 일반적으로 공격자가 컴퓨터를 보트로 감염시키고 나면, 감염된 컴퓨터가 IRC 서버에 연결된 후 특정 채널을 열고 스팸 전자 메일을 보내라는 명령을 기다리게 됩니다. Mail Protection에서는 알 수 없는 봇의 스팸 전자 메일을 일반 전자 메일과 구분하기 위해 보내는 전자 메일에 대해 SMTP 서버와 전자 메일 보낸 사람이 허용된 서버 목록 및 보낸 사람 목록에 포함되어 있는지 여부를 검사합니다. 목록에 없을 경우 보내는 전자 메일이 차단되어 전자 메일이 전송되지 않습니다. 차단된 전자 메일은 대화 상자에 표시됩니다. (옵션은 고급 모드에서만 사용 가능)

참고

AntiBot 기능은 Mail Protection의 보내는 전자 메일 검사가 사용하도록 설정된 경우에만 사용할 수 있습니다([Mail Protection > 검사](#)에서 보내는 전자 메일 검사 옵션 참조).

허용된 서버

이 목록의 모든 서버는 Mail Protection으로부터 전자 메일을 보내도록 허용됩니다. 이러한 서버로 보낸 전자 메일은 Mail Protection을 통해 차단되지 **않습니다**. 이 목록에 서버가 하나도 포함되지 않은 경우 보내는 전자 메일을 보내는 데 사용되는 SMTP 서버를 검사하지 않습니다. 이 목록에 항목이 있는 경우 Mail Protection에서 이 목록에 포함되지 않은 SMTP 서버로 전송되는 전자 메일을 차단합니다.

입력란

이 입력란에는 전자 메일을 보내는 데 사용하는 **SMTP** 서버의 **IP** 주소 또는 호스트 이름을 입력합니다.

참고

사용자 계정을 만든 날짜 아래에서 전자 메일 프로그램이 전자 메일을 보내는 데 사용한 **SMTP** 서버에 대한 자세한 정보를 볼 수 있습니다.

추가

이 버튼을 사용하여 입력란에 지정된 서버를 허용된 서버 목록에 포함할 수 있습니다.

삭제

이 버튼은 허용된 서버 목록에서 강조 표시된 항목을 삭제합니다. 항목을 선택하지 않으면 이 버튼이 비활성화됩니다.

모두 선택 취소

이 버튼은 허용된 서버 목록에서 모든 항목을 삭제합니다.

허용된 보낸 사람

이 목록의 모든 서버는 **Mail Protection**으로부터 전자 메일을 보내도록 허용됩니다. 이러한 서버로 보낸 전자 메일은 **Mail Protection**을 통해 차단되지 **않습니다**. 이 목록에 보낸 사람이 한 명도 없는 경우 보내는 전자 메일을 보내는 데 사용된 전자 메일 주소를 검사하지 않습니다. 이 목록에 항목이 있는 경우 **Mail Protection**에서 이 목록에 포함되지 않은 보낸 사람이 보내는 전자 메일을 차단합니다.

입력란

이 상자에는 전자 메일 보낸 사람 주소를 입력합니다.

추가

이 버튼을 사용하여 입력란에 지정된 보낸 사람을 허용된 보낸 사람 목록에 포함할 수 있습니다.

삭제

이 버튼은 허용된 보낸 사람 목록에서 강조 표시된 항목을 삭제합니다. 항목을 선택하지 않으면 이 버튼이 비활성화됩니다.

모두 선택 취소

이 버튼은 허용된 보낸 사람 목록에서 모든 항목을 삭제합니다.

12.7.2 일반

예외

검사 예외

이 테이블은 **Mail Protection**의 검사로부터 제외되는 전자 메일 주소 목록(허용 목록)을 표시합니다.

참고

받는 전자 메일의 경우 **Mail Protection**에서만 예외 목록이 사용됩니다.

검사 예외

입력란

이 상자에는 검사하지 않을 전자 메일 주소 목록에 추가할 전자 메일 주소를 입력합니다. 설정에 따라 해당 전자 메일 주소에 대해 **Mail Protection**에서 이후에 더 이상 검사하지 않습니다.

참고

전자 메일 주소를 입력할 때 임의의 문자 수를 나타내는 *와 단일 문자를 나타내는 ?를 와일드카드로 사용할 수 있습니다. 하지만 와일드카드는 스팸 포함 여부를 검사하지 않는 전자 메일 주소에 대해서만 사용할 수 있습니다. **맬웨어 제외 목록** 상자를 선택하여 와일드카드를 포함하는 주소를 맬웨어 검사에서 제외시키려 할 경우 오류 메시지가 표시됩니다. 와일드카드가 사용된 주소를 입력할 때 지정된 문자 순서와 전자 메일 주소의 구조(*@*.*)가 일치해야 합니다.

경고

와일드카드 사용에 대한 예를 참고하십시오. 와일드카드는 선택적으로만 사용하도록 하며 와일드카드를 포함하는 전자 메일 주소를 스팸 허용 목록에 추가할 경우에는 각별히 유의하십시오.

예: 전자 메일 주소에서 와일드 카드 사용(스팸 허용 목록)

- virus@avira.* / = 이 주소에 해당하는 모든 최상위 도메인의 모든 전자 메일: virus@avira.de, virus@avira.com, virus@avira.net 등.
- *@avira.com = **avira.com** 도메인에서 전송된 모든 전자 메일: info@avira.com, virus@avira.com, kontakt@avira.com, employee@avira.com
- info@*.com = 최상위 도메인이 **com**이고 주소가 **info**인 모든 전자 메일. 2 수준의 도메인은 info@name1.com, info@name2.com 등이 될 수 있습니다.

추가

이 버튼을 사용하면 입력란에 입력한 전자 메일 주소를 검사하지 않을 전자 메일 주소의 목록에 추가할 수 있습니다.

삭제

이 버튼은 강조 표시된 전자 메일 주소를 목록에서 삭제합니다.

전자 메일 주소

더 이상 검사하지 않을 전자 메일입니다.

맬웨어

이 옵션을 사용하면 전자 메일 주소에 대해 맬웨어 포함 여부를 더 이상 검사하지 않습니다.

스팸

이 옵션을 사용하면 전자 메일 주소에 대해 스팸 포함 여부를 더 이상 검사하지 않습니다.

위로

이 버튼을 사용하면 강조 표시된 전자 메일 주소를 목록에서 위쪽으로 이동할 수 있습니다. 목록에 강조 표시된 항목이 없거나 강조 표시된 주소가 목록의 첫 번째 항목인 경우에는 이 버튼을 사용할 수 없습니다.

아래로

이 버튼을 사용하면 강조 표시된 전자 메일 주소를 목록에서 아래쪽으로 이동할 수 있습니다. 목록에 강조 표시된 항목이 없거나 강조 표시된 주소가 목록의 마지막 항목인 경우에는 이 버튼을 사용할 수 없습니다.

Outlook 주소록 가져오기

이 버튼을 사용하면 MS Outlook 전자 메일 프로그램의 주소록에 있는 전자 메일 주소를 예외 목록으로 가져올 수 있습니다. 가져온 전자 메일 주소에 대해 스팸 포함 여부를 검사하지 않습니다.

Outlook Express 주소록 가져오기(Windows XP)/Windows Mail 주소록 가져오기(Windows Vista, Windows 7)

이 버튼을 사용하여 MS Outlook Express 또는 Windows Mail 전자 메일 프로그램의 주소록에 있는 전자 메일 주소를 예외 목록으로 가져올 수 있습니다. 가져온 전자 메일 주소에 대해 스팸 포함 여부를 검사하지 않습니다.

캐시

Mail Protection 캐시에는 제어 센터의 **Mail Protection**에 통계 데이터로 표시되는 검사한 전자 메일에 관한 데이터가 포함되어 있습니다. (옵션은 고급 모드에서만 사용 가능)

캐시에는 받는 전자 메일의 복사본도 보관되어 있습니다. 이러한 전자 메일은 스팸 방지 모듈의 학습 기능(**정상 전자 메일 - 학습용**, **스팸 - 학습용**)에도 사용할 수 있습니다.

참고

받는 전자 메일을 캐시 안에 백업하려면 스팸 방지 모듈을 활성화해야 합니다.

캐시의 최대 전자 메일 수

이 항목은 Mail Protection에서 캐시에 저장하는 최대 전자 메일 수를 설정하는 데 사용됩니다. 전자 메일은 가장 오래된 것부터 삭제됩니다.

전자 메일의 최대 저장 일 수

이 상자에는 최대 전자 메일 보관 기간을 일 단위로 입력합니다. 이 기간이 경과되면 전자 메일이 캐시에서 제거됩니다.

캐시 비우기

이 버튼을 클릭하면 캐시에 저장된 전자 메일이 삭제됩니다.

바닥글

바닥글에서는 보내는 전자 메일에 표시되는 전자 메일 바닥글을 구성할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

이 기능을 사용하려면 보내는 전자 메일에 대한 Mail Protection 검사를 활성화해야 합니다(**구성 > Mail Protection > 검사**에서 **보내는 전자 메일 검사(SMTP)** 옵션 참조). 정의된 Avira Mail Protection 바닥글을 사용하여 바이러스 방지 프로그램이 보낸 전자 메일을 검사했음을 확인할 수 있습니다. 또한 사용자 정의 바닥글을 삽입할 수 있습니다. 두 바닥글 옵션을 모두 사용하는 경우에는 Avira Mail Protection 바닥글이 사용자 정의 텍스트 앞에 옵니다.

전송할 전자 메일의 바닥글

Mail Protection 바닥글 첨부

이 옵션을 사용하면 보낸 전자 메일의 메시지 텍스트 아래에 Avira Mail Protection 바닥글이 표시됩니다. Avira Mail Protection 바닥글은 Avira Mail Protection이 보낸 전자 메일에서 바이러스 및 사용자 동의 없이 설치된 프로그램을 검사했으며 알 수 없는 붓에서 보내는 것이 아님을 확인합니다. Avira Mail Protection 바닥글에 "**Avira Mail**

Protection [제품 버전][검색 엔진의 이니셜 및 버전 번호][바이러스 정의 파일의 이니셜 및 버전 번호]을(를) 사용하여 검사했습니다."라는 텍스트가 포함됩니다.

다음 바닥글 첨부

이 옵션을 사용하면 입력란에 삽입한 텍스트가 보낸 전자 메일에 바닥글로 표시됩니다.

입력란

이 입력란에는 보낸 전자 메일에 바닥글로 표시할 텍스트를 삽입할 수 있습니다.

AntiSpam

Avira Mail Protection 서비스는 전자 메일과 해당 첨부 파일에 바이러스 및 사용자 동의 없이 설치된 프로그램이 있는지 검사합니다. 또한 스팸 전자 메일로부터 사용자를 안정적으로 보호할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

AntiSpam 모듈 사용

이 옵션을 사용하면 Mail Protection의 스팸 방지 기능이 활성화됩니다.

전자 메일 주소 표시

이 옵션을 사용하면 스팸 전자 메일이 발견될 때 원래 제목 줄에 메모가 추가됩니다.

간단히

스팸 또는 피싱 전자 메일을 받으면 [스팸] 또는 [피싱]이라는 단어가 추가됩니다. 이 옵션은 기본 설정으로 선택됩니다.

자세히

스팸 또는 피싱 전자 메일의 제목 줄 앞에 해당 메시지가 스팸일 가능성이 높다는 경고 내용이 추가됩니다.

로깅 사용

이 옵션을 사용하면 Mail Protection에서 특수한 스팸 방지 보고서 파일을 만듭니다.

실시간 차단 목록 사용

이 옵션을 사용하면 "차단 목록"을 실시간으로 쿼리합니다. 차단 목록은 의심스러운 출처의 전자 메일을 스팸으로 분류하는 데 필요한 추가 정보를 제공합니다.

시간 초과: n초

n초 후에도 차단 목록의 정보를 사용할 수 없으면 차단 목록 쿼리 시도가 중단됩니다.

학습 데이터베이스 지우기

이 버튼을 클릭하면 학습 데이터베이스가 삭제됩니다.

보내는 메일의 받는 사람을 허용 목록에 자동으로 추가

이 옵션을 사용하면 보내는 전자 메일의 받는 사람 주소가 스팸 허용 목록(**Mail Protection > 일반 > 예외**에서 정의한 스팸 여부가 검사되지 않는 전자 메일 목록)에 자동으로 추가됩니다. 스팸 허용 목록에 있는 주소에서 전송한, 받는 전자 메일에 대해서는 스팸 포함 여부를 검사하지 않습니다. 하지만 바이러스 및 맬웨어 포함 여부는 검사합니다. 이 옵션은 기본적으로 사용되지 않습니다.

참고

이 옵션은 **Mail Protection**의 보내는 전자 메일 검사가 사용하도록 설정된 경우에만 사용할 수 있습니다(**Mail Protection > 검사**에서 보내는 전자 메일 검사 옵션 참조).

12.7.3 보고서

Mail Protection에는 사용자 또는 관리자에게 검색 유형 및 방식에 대한 정확한 정보를 제공하기 위한 광범위한 로깅 기능이 포함됩니다. (옵션은 고급 모드에서만 사용 가능)

보고

이 그룹에서는 보고서 파일의 콘텐츠를 결정할 수 있습니다.

해제

이 옵션을 사용하면 **Mail Protection**에서 로그를 만들지 않습니다. 평가판을 실행하여 여러 바이러스나 사용자 동의 없이 설치된 프로그램을 테스트하려는 경우처럼 예외적인 상황이 아니면 로깅 기능을 해제하지 않는 것이 좋습니다.

기본값

이 옵션을 사용하면 **Mail Protection**에서 바이러스 발견, 알림 및 오류 관련 중요 정보를 보고서 파일에 기록하고 중요 항목의 보다 확실한 전달을 위해 중요도가 낮은 정보는 무시합니다. 이 옵션은 기본 설정으로 선택됩니다.

확장

이 옵션을 사용하면 **Mail Protection**에서 덜 중요한 정보도 보고서 파일에 기록합니다.

완료

이 옵션을 사용하면 **Mail Protection**에서 모든 정보를 보고서 파일에 기록합니다.

보고서 파일 제한

nMB로 크기 제한

이 옵션을 사용하면 보고서 파일을 특정 크기로 제한할 수 있습니다. 허용되는 값은 1~100MB입니다. 보고서 파일의 크기를 제한하여 시스템 리소스 사용을 최소화하면 약 50KB의 추가 공간이 확보됩니다. 로그 파일의 크기가 지정된 크기를 50KB 이상 초과하는 경우에는 (지정된 크기 - 50KB)의 크기가 될 때까지 오래된 항목이 삭제됩니다.

줄이기 전에 보고서 파일 백업

이 옵션을 사용하면 보고서 파일의 크기를 줄이기 전에 보고서 파일을 백업합니다.

보고서 파일에 구성 쓰기

이 옵션을 사용하면 Mail Protection 구성이 보고서 파일에 기록됩니다.

참고

보고서 파일 제한을 지정하지 않은 경우 보고서 파일이 100MB에 도달하면 새 보고서 파일이 자동으로 생성됩니다. 이전 보고서 파일의 백업이 생성됩니다. 이전 보고서 파일에 대해 최대 세 개 백업이 저장됩니다. 가장 오래된 백업부터 삭제됩니다.

12.8 자녀 보호

Avira의 *자녀 보호* 기능을 사용하면 컴퓨터를 사용하는 자녀 또는 다른 사람에게 안전한 인터넷 환경을 제공할 수 있습니다.

- **Safe Browsing** 기능을 사용하면 컴퓨터의 각 Windows 사용자에게 역할을 할당할 수 있습니다. 모든 역할에 대해 허용하거나 거부할 인터넷 콘텐츠의 범주나 URL을 정의하고 일일 사용 시간대 또는 시간 제한을 정의할 수 있습니다.

관련 항목:

- [Safe Browsing](#) 정보

12.8.1 Safe Browsing

Safe Browsing 기능을 사용하여 원하지 않거나 불법적인 인터넷 콘텐츠를 필터링하고 인터넷 사용 시간을 제한할 수 있습니다. **Safe Browsing** 기능은 *자녀 보호* 구성 요소의 일부입니다.

컴퓨터의 Windows 사용자 계정에 사용자 역할을 할당할 수 있습니다. 각 사용자 역할에는 다음 조건의 규칙 집합이 포함됩니다.

- 허용 및 차단된 URL(인터넷 주소)
- 금지된 URL 범주

- 인터넷 사용 시간 및 허용된 평일 사용 기간(필요한 경우)

특정한 범주에 따라 인터넷 콘텐츠를 차단하기 위해 Avira에서는 웹 페이지의 콘텐츠에 따라 URL을 필터링하는 강력한 URL을 사용합니다. URL 필터 목록은 1시간마다 업데이트, 조정 및 확장됩니다. 어린이, 청소년 및 성인 역할이 관련된 금지 범주로 사전 구성되어 있습니다. 인터넷 사용은 5분 이상 지속되는 인터넷 요청을 기반으로 하여 로그에 기록됩니다.

Safe Browsing을 사용하도록 설정한 경우에는, 사용자가 요청하는 모든 웹 페이지를 사용자 역할에 따라 필터링합니다. 웹 페이지가 차단되면 브라우저에 메시지가 표시됩니다. 허용된 사용 시간을 초과했거나 허용 시간을 벗어나 사용할 경우, 요청된 웹 사이트가 차단되고 브라우저에 메시지가 표시됩니다.

경고

Safe Browsing 기능을 사용하려면 **Web Protection** 서비스를 사용하도록 설정해야 합니다.

경고

Safe Browsing을 사용하도록 설정한 경우 Avira 제품의 구성을 암호로 보호하십시오. 구성을 암호로 보호하지 않으면, 컴퓨터의 모든 사용자가 **Safe Browsing** 설정을 변경하거나 사용하지 않도록 설정할 수 있습니다. 암호 보호는 [구성 > 일반 > 암호](#) 아래에서 설정합니다.

관련 항목:

- [Safe Browsing 사용](#)
- [Safe Browsing 역할 할당](#)
- [Safe Browsing 구성](#)

Safe Browsing 사용

- ▶ Avira 제어 센터에서 탐색 막대의 상태를 클릭합니다.

Safe Browsing 기능을 사용하려면 **Web Protection** 서비스를 사용하도록 설정해야 합니다.

- ▶ 필요한 경우 상태 보기에서 *인터넷 보호* 아래에 있는 **Web Protection** 옆의 빨간색 스위치를 클릭하여 이 서비스를 활성화합니다.

Web Protection을 활성화하면 상태가 녹색(I)이어야 합니다.

상태 보기에서 옆에 있는 빨간색 스위치를 클릭하여 **Safe Browsing** 서비스를 활성화합니다.

Safe Browsing을 활성화하면 상태가 녹색(I)이어야 합니다.

- ▶ 자녀 또는 다른 사용자에 대한 **Safe Browsing** 프로필을 구성하려면, **상태** 보기에서 **Safe Browsing** 옆의 구성 버튼을 클릭합니다.

관련 항목:

- [Safe Browsing](#) 정보
- [Safe Browsing](#) 역할 할당
- [Safe Browsing](#) 구성

Safe Browsing 역할 할당

전제 조건:

- ✓ Avira를 설치한 컴퓨터를 사용하여 각 사용자에게 별도의 **Windows** 계정을 할당해야 합니다. 각 **Windows** 사용자 계정에 **Safe Browsing** 역할을 할당할 수 있습니다.
- ✓ Avira 제품에서 **Safe Browsing** 기능을 사용하도록 설정합니다.
- ✓ 각 역할에 대한 설정을 확인하고 사용자에게 역할을 할당하기 전에 이를 변경합니다.

- ▶ **상태** 보기에서 **Safe Browsing** 옆의 구성 버튼을 클릭합니다.
- ▶ **사용자 선택** 드롭다운 목록에서 역할을 할당할 사용자 이름을 선택합니다.
이 목록에는 컴퓨터에 구성된 **Windows** 사용자 계정이 포함됩니다.
- ▶ 추가 버튼을 클릭합니다.
↳ 사용자가 목록에 추가됩니다.

Avira Internet Security에는 다음과 같은 사전 구성된 사용자 역할이 함께 제공됩니다.

- 어린이
- 청소년
- 성인

기본적으로 목록에 사용자를 추가할 때 할당되는 역할은 **어린이**입니다.

- ▶ 각 사용자의 역할을 클릭하여 다른 역할을 할당할 수 있습니다.

참고

Safe Browsing을 사용할 경우, **Safe Browsing**을 구성할 때 역할을 할당하지 않은 컴퓨터의 기본 사용자에게는 **어린이** 역할이 할당됩니다. **기본** 사용자의 역할은 변경할 수도 있습니다.

- ▶ **적용**을 클릭하여 구성을 저장합니다.

관련 항목:

- [역할 속성 변경](#)
- [역할 추가 또는 제거](#)

역할 속성 변경

- ▶ 상태 보기에서 **Safe Browsing** 옆의 구성 버튼을 클릭합니다.
- ▶ 필요한 경우 옆에 있는 녹색 스위치를 클릭하여 **고급 모드**를 활성화합니다.
고급 모드를 활성화하면 해당 상태가 노란색(I)으로 표시됩니다.
↳ **Safe Browsing** 구성 창에 **역할** 옵션이 나타납니다.
- ▶ 변경할 역할의 이름(예를 들어 **청소년**)을 클릭한 다음 **변경** 버튼을 클릭합니다.
↳ 선택한 역할에 대한 **속성** 창이 나타납니다.
- ▶ 원하는 대로 변경한 다음 **확인**을 클릭합니다.

관련 항목:

- [역할 속성](#)
- [Safe Browsing 구성](#)

역할 추가 또는 제거

- ▶ 상태 보기에서 **Safe Browsing** 옆의 구성 버튼을 클릭합니다.
- ▶ 필요한 경우 옆에 있는 녹색 스위치를 클릭하여 **고급 모드**를 활성화합니다.
고급 모드를 활성화하면 해당 상태가 노란색(I)으로 표시됩니다.
↳ **Safe Browsing** 구성 창에 **역할** 옵션이 나타납니다.
- ▶ 역할을 삭제하려면 역할의 이름(예를 들어 **청소년**)을 클릭한 다음 **제거** 버튼을 클릭합니다.

참고

사용자에게 할당된 역할을 삭제할 수 없습니다.

- ▶ 새 역할을 추가하려면 입력 항목에 역할 이름을 입력하고(최대 30자) **새로 만들기** 버튼을 클릭합니다.
- ▶ 역할 목록에서 새 역할의 이름을 선택하고 **변경** 버튼을 클릭하여 해당 속성을 편집합니다.

관련 항목:

- [Safe Browsing 구성](#)
- [역할 속성](#)

- **Safe Browsing 역할 할당**

Safe Browsing에 대한 암호를 할당한 경우에는 구성이 숨겨지고 **암호 사용** 버튼이 표시됩니다.

암호 사용

"**Safe Browsing**" 구성을 사용하려면 "**암호 사용**" 버튼을 누르고 "**암호 입력**" 창에 암호를 입력합니다.

Safe Browsing 사용

이 옵션을 선택하면 "**Safe Browsing**" 기능에 등록된 사용자에게 할당된 역할을 기반으로 하여 사용자가 인터넷을 탐색하는 동안 요청하는 모든 웹 페이지를 검사합니다. 요청한 웹 페이지가 할당된 역할 내에서 차단된 페이지로 분류된 경우 해당 페이지는 차단됩니다.

참고

Safe Browsing을 사용할 경우, **Safe Browsing**을 구성할 때 역할을 할당하지 않은 컴퓨터의 기본 사용자에게는 **어린이** 역할이 할당됩니다. 기본 사용자의 역할은 변경할 수 있습니다.

설치 후 **어린이**, **청소년** 및 **성인** 사용자 역할이 만들어집니다. 미리 구성된 역할에 대해서는 인터넷 사용 시간 제한이 적용되지 않습니다.

사용자 선택

사용자 드롭다운 목록

이 목록에는 시스템의 모든 사용자가 포함되어 있습니다.

추가

이 버튼을 사용하여 보호되는 사용자 목록에 선택한 사용자를 추가할 수 있습니다.

삭제

이 버튼은 목록에서 선택한 항목을 삭제합니다.

사용자 역할 목록

이 목록은 역할이 할당되어 있는 추가된 모든 사용자를 표시합니다. 사용자를 추가하면 프로그램에서는 기본적으로 **어린이** 역할을 할당합니다. 표시된 역할을 마우스로 클릭하면 다른 역할로 전환할 수 있습니다.

참고

기본 사용자는 삭제할 수 없습니다.

역할(옵션은 고급 모드에서만 사용 가능)

입력란

이 항목에는 사용자 역할에 추가할 역할의 이름을 입력할 수 있습니다.

변경

"변경" 버튼을 사용하여 선택된 역할을 구성할 수 있습니다. 역할에 대한 차단 및 허용된 URL과 범주에 따라 금지되는 웹 콘텐츠를 정의할 수 있는 대화 상자가 나타납니다.
([역할 속성 참조](#))

새로 만들기

이 버튼을 사용하면 입력란에 입력한 역할을 사용 가능 역할 목록에 추가할 수 있습니다.

제거

이 버튼은 목록에서 강조 표시된 역할을 삭제합니다.

목록

이 목록은 추가된 모든 역할을 표시합니다. 표시된 역할을 더블클릭하면 역할을 정의할 수 있는 대화 상자가 열립니다.

참고

사용자에게 이미 할당된 역할은 삭제할 수 없습니다.

관련 항목:

- [Safe Browsing](#) 정보
- [역할 속성](#)
- [사용 시간](#)
- [사용 기간](#)

역할 속성

속성 창에서는 인터넷 사용과 관련하여 선택한 역할을 정의할 수 있습니다. (옵션은 고급 모드에서만 사용 가능)

URL에 대한 액세스를 명시적으로 허용하거나 금지할 수 있습니다. 사용자 선택에 따라 웹 콘텐츠의 특정 범주를 차단할 수 있습니다. 또한 인터넷 사용 시간을 제한할 수도 있습니다.

다음 URL에 대한 액세스 제어

이 목록에는 **차단** 또는 **허용** 규칙이 할당되어 있는 추가된 모든 URL이 표시됩니다. URL을 추가하면 이 프로그램에서는 기본적으로 **차단** 규칙을 할당합니다. 규칙을 클릭하여 할당된 규칙을 전환할 수 있습니다.

URL 추가

자녀 보호 기능을 통해 제어할 URL을 지정하는 항목입니다. 앞이나 뒤의 점으로 도메인 수준을 표시하여 URL의 일부를 지정할 수 있습니다. 예를 들어 도메인의 모든 페이지와 모든 하위 도메인을 지정하려면 `.domainname.com`을 지정합니다. 최상위 도메인(`.com` 또는 `.net`)을 사용하는 모든 웹 사이트를 나타내려면 뒤에 점을 추가합니다(`domainname.`). 앞이나 뒤에 점이 없는 문자열을 지정하면 문자열은 최상위 도메인으로 해석됩니다(예: `net`은 모든 **NET** 도메인(`www.domain.net`)을 나타냄). 모든 수의 문자를 나타내는 와일드카드 `*`도 사용할 수 있습니다. 와일드카드와 함께 선행 또는 후행 점을 사용하여 도메인 수준을 나타낼 수도 있습니다.

참고

URL 규칙에는 지정된 도메인 레이블 수에 따라 우선 순위가 부여됩니다. 지정된 도메인의 레이블이 많을수록 규칙의 우선 순위가 더 높습니다. 예:

URL: `www.avira.com` - 규칙: 허용

URL: `.avira.com` - 규칙: 차단

규칙 집합은 `www.avira.com` 도메인의 모든 URL을 허용합니다. `forum.avira.com` URL은 차단됩니다.

참고

`.` 또는 `*`는 모든 URL을 포함합니다. 예를 들어 다음 규칙 집합에서처럼 **어린이** 역할에 대해서는 몇 개의 명시적으로 지정된 웹 페이지만 해제하려고 할 때 이 세부 정보를 사용할 수 있습니다.

URL: `*` 또는 `.` 규칙: 차단

URL: `kids.yahoo.com` - 규칙: 허용

URL: `kids.nationalgeographic.com` - 규칙: 허용

이 규칙 집합은 도메인이 `kids.yahoo.com` 및 `kids.nationalgeographic.com`인 URL을 제외한 모든 URL을 차단합니다.

추가

이 버튼을 사용하면 입력한 URL을 제어되는 URL 목록에 추가할 수 있습니다.

삭제

이 버튼은 제어되는 URL 목록에서 강조 표시된 URL을 삭제합니다.

다음 범주에 속하는 URL에 대한 액세스 차단

이 옵션을 사용하면 범주 목록에서 선택한 범주에 속하는 웹 콘텐츠가 차단됩니다.

허용된 사용 시간

허용된 사용 시간은 구성 중인 역할의 인터넷 사용 시간 제한을 설정할 수 있는 대화 상자를 표시합니다. 주 또는 월을 기준으로 인터넷 사용을 지정하거나 평일과 주말을 구분할 수 있습니다. 추가 대화 상자에서는 정확한 평일 사용 기간을 지정할 수 있습니다. [사용 시간](#)을 참조하십시오.

제어할 URL의 예

- `www.avira.com` -또는- `www.avira.com/*`
= 도메인이 `www.avira.com`: `www.avira.com/en/pages/index.php`,
`www.avira.com/en/support/index.html`, `www.avira.com/en/download/index.html`인
모든 URL을 포함합니다.
도메인이 `www.avira.de`인 URL은 포함되지 않습니다.
- `avira.com` -또는- `*.avira.com`
= 2차 및 최상위 수준 도메인 `avira.com`을 사용하는 모든 URL 포함. 여기에는
.avira.com의 모든 기존 하위 도메인(`www.avira.com`, `forum.avira.com` 등)이
포함됩니다.
- `avira.` -또는- `*.avira.*`
= 2차 수준 도메인 `avira`가 포함된 모든 URL을 포함합니다. .avira의 모든 기존
최상위 도메인 또는 하위 도메인을 포함합니다(`www.avira.com`, `www.avira.de`,
`forum.avira.com` 등).
- `.*domain*.*`
문자열 `domain`이 있는 2차 수준 도메인이 포함된 모든 URL을
포함합니다(`www.domain.com`, `www.new-domain.de`, `www.sample-domain1.de` 등).
- `net` -또는- `*.net`
= 최상위 도메인 `net`이 포함된 모든 URL을 포함합니다(`www.name1.net`,
`www.name2.net` 등).

관련 항목:

- [Safe Browsing](#) 정보
- [Safe Browsing](#) 구성
- [사용 시간](#)
- [사용 기간](#)

사용 시간

사용 시간 창에서는 사용자 역할에 대한 최대 인터넷 사용 시간을 설정할 수 있습니다. 인터넷 사용 로그는 5분 이상 지속된 인터넷 요청을 기반으로 합니다. 역할에 필요한 최대 검색 시간은 주 또는 월별로 지정하거나, 평일과 주말에 대해 서로 다르게 지정할 수 있습니다.

인터넷 사용 시간 제한

이 옵션을 사용하면 역할이 할당된 모든 컴퓨터 사용자의 인터넷 사용 시간을 제한할 수 있습니다. 허용된 사용 시간이 초과하면 컴퓨터 사용자의 웹 사이트 요청이나 액세스가 차단됩니다. 그리고 웹 브라우저에 경고가 나타납니다.

주, 월, 요일(월-금, 토-일)별 시간 제한

필요한 사용 시간은 슬라이더나 입력란 오른쪽에 있는 화살표 키를 사용하여 조정할 수 있습니다. 또한 시간 박스에 직접 사용 시간을 입력할 수도 있습니다. 이때 시간 지정에 대한 특정 형식에 주의하십시오.

여러 개의 사용 시간 지정은 프로그램에서 조정되지 않습니다. 프로그램에서는 언제든지 허용되는 최저값을 사용하여 사용 시간을 제한합니다.

정확한 사용 기간

정확한 사용 기간 버튼을 사용하면 대화 상자에서 정의된 최대 사용 시간에 대해 하루 중 사용 가능한 시간대를 지정할 수 있습니다. [사용 기간](#)을 참조하십시오.

관련 항목:

- [Safe Browsing](#) 정보
- [Safe Browsing](#) 구성
- [역할 속성](#)
- [사용 기간](#)

사용 기간

사용 기간 창에서 선택된 역할에 허용된 사용 시간을 설정할 수 있습니다. 하루 중 인터넷을 사용할 수 있는 특정 시간대를 정의할 수 있습니다.

지정된 시간에만 인터넷 사용 허용

이 옵션을 사용하면 구성된 역할이 할당된 모든 컴퓨터 사용자가 하루 중 인터넷을 '검색'할 수 있는 시간을 설정할 수 있습니다. 사용자가 지정된 시간 이외에 인터넷을 사용하려고 하면 요청된 웹 사이트가 차단됩니다. 이 경우 웹 브라우저에 메시지가 나타납니다.

- ▶ 하루 중 인터넷을 사용 시간대를 지정하려면 필요한 시간 항목을 강조 표시합니다.
허용된 시간과 금지된 시간 간격을 정의할 때 다음 옵션을 사용할 수 있습니다.

- **검색 허용 시간을 정의하려면:** 강조 표시되지 않은 시간 항목을 클릭하거나 강조 표시되지 않은 시간 항목 뒤로 마우스 왼쪽 버튼을 끕니다.
- **검색 금지 시간을 정의하려면:** 강조 표시된 시간 항목을 클릭하거나 강조 표시된 시간 항목 뒤로 마우스 왼쪽 버튼을 끕니다.
- ▶ 요일의 행에서 강조 표시되거나 강조 표시되지 않은 영역을 오른쪽 클릭하면 해당 요일에 대해 정의된 간격이 포함된 세부 정보 창이 표시됩니다. 예:
00:00부터 11:00까지 인터넷 사용이 차단됩니다.

관련 항목:

- [Safe Browsing](#) 정보
- [Safe Browsing](#) 구성
- 역할 속성
- 사용 시간

12.9 모바일 보호

12.9.1 모바일 보호

Avira는 사용자의 컴퓨터 시스템을 맬웨어와 바이러스로부터 보호할 뿐만 아니라 **Android** 운영 체제를 실행하는 스마트폰을 손실과 도난으로부터 방지합니다. **Avira Free Android Security**를 사용하면 원하지 않는 전화나 **SMS**를 차단할 수 있습니다. 통화 기록, **SMS** 기록 및 연락처 목록의 전화 번호를 차단 목록에 추가하거나 차단할 연락처를 직접 만들 수 있습니다.

다음 웹 사이트에서 자세한 내용을 확인할 수 있습니다.

<http://www.avira.com/android>

12.10 일반

12.10.1 위협 범주

확장된 위협 범주의 선택(옵션은 고급 모드에서만 사용 가능)

Avira 제품은 컴퓨터 바이러스로부터 사용자 시스템을 보호합니다. 또한 다음과 같은 확장된 위협 범주에 따라 시스템을 검사할 수 있습니다.

- 애드웨어
- 애드웨어/스파이웨어
- 응용 프로그램

- 백도어 클라이언트
- 다이얼러
- 이중 확장명 파일
- 사기성 소프트웨어
- 게임
- 장난 프로그램
- 피싱
- 개인 도메인을 위반한 프로그램
- 비정상적인 런타임 압축 프로그램

관련 상자를 클릭하면 선택한 유형이 사용되거나(확인 표시 있음) 사용되지 않습니다(확인 표시 없음).

모두 선택

이 옵션을 사용하면 모든 유형이 사용됩니다.

기본값

이 버튼은 미리 정의된 기본값을 복원합니다.

참고

유형 중 하나를 사용하지 않으면 관련 프로그램 유형으로 인식되는 파일이 더 이상 표시되지 않습니다. 보고서 파일에 항목이 작성되지 않습니다.

12.10.2 고급 보호 기능

ProActiv(옵션은 고급 모드에서만 사용 가능)

ProActiv 사용

이 옵션을 선택하면 시스템의 프로그램을 모니터링하고 의심스러운 활동을 확인합니다. 일반적인 맬웨어 동작이 검색되면 메시지가 표시됩니다. 프로그램을 차단하거나 "무시"를 선택하여 프로그램을 계속 사용할 수 있습니다. 신뢰할 수 있는 프로그램으로 분류된 프로그램, 허용된 응용 프로그램 필터에 기본적으로 포함된 신뢰할 수 있고 서명된 프로그램 및 허용된 프로그램으로 응용 프로그램 필터에 추가한 모든 프로그램은 모니터링 프로세스에서 제외됩니다.

ProActiv는 아직 바이러스 정의나 추론이 없는 새로운 위협 및 알려지지 않은 위협으로부터 보호합니다. **ProActiv** 기술은 **Real-Time Protection** 구성 요소에 통합되어 있으며 수행되는 프로그램 작업을 관찰하고 분석합니다. 프로그램의 동작을 일반적인 맬웨어 동작 패턴, 즉

작업의 유형 및 작업 순서와 비교합니다. 프로그램이 일반적인 맬웨어 동작을 보이는 경우에는 바이러스 탐지로 취급됩니다. 프로그램을 차단하거나 알림을 무시하고 프로그램을 계속 사용할 수 있습니다. 프로그램을 차단하거나 알림을 무시하고 프로그램을 계속 사용할 수 있습니다. **항상 차단** 명령을 사용하여 프로그램을 차단 프로그램에 대한 응용 프로그램 필터에 추가할 수 있습니다.

ProActiv 구성 요소에서는 Avira 맬웨어 연구 센터에서 개발한 규칙 집합을 사용하여 의심스러운 동작을 식별합니다. 규칙 집합은 Avira 데이터베이스에서 제공됩니다. ProActiv는 모든 의심스러운 프로그램에 대한 정보를 Avira 데이터베이스로 보내서 기록합니다. Avira를 설치할 때 Avira 데이터베이스로의 데이터 전송을 해제할 수 있습니다.

참고

ProActiv 기술은 64비트 시스템에서는 아직 사용할 수 없습니다.

Protection Cloud(옵션은 고급 모드에서만 사용 가능)

Protection Cloud 사용

의심스러운 모든 파일의 핑거프린트는 동적 온라인 검사를 위해 Protection Cloud로 전송됩니다. 실행 파일은 즉시 미감염, 감염 또는 알 수 없음으로 식별됩니다.

Protection Cloud는 모든 사용자에게 대해 시도된 사이버 공격을 감시하기 위한 중앙 위치의 역할을 합니다. 컴퓨터가 액세스하는 파일을 클라우드에 저장된 파일의 핑거프린터와 비교합니다. 클라우드에서 수행되는 검사가 많을수록 바이러스 백신 응용 프로그램에 필요한 프로세싱 파워가 줄어듭니다.

빠른 시스템 검사 작업이 실행될 때는 맬웨어의 공격 대상이 되는 경우가 많은 파일 위치의 목록이 생성됩니다. 이 목록에는 실행 중인 프로세스, 시작 시 실행되는 프로그램 및 서비스가 포함됩니다. 각 파일의 핑거프린트가 생성되어 Protection Cloud로 전송된 다음, "미감염" 또는 "맬웨어"로 분류됩니다. 알 수 없는 프로그램 파일은 분석을 위해 Protection Cloud로 업로드됩니다.

의심되는 파일을 Avira에 보낼 때 수동으로 확인

Protection Cloud로 전송해야 하는 의심스러운 파일의 목록을 볼 수 있으며, 전송할 파일을 선택할 수 있습니다.

차단된 응용 프로그램

차단할 응용 프로그램에서는 유해한 것으로 분류한 응용 프로그램과 기본적으로 Avira ProActiv에서 차단할 응용 프로그램을 입력할 수 있습니다. 추가된 응용 프로그램은 컴퓨터 시스템에서 실행할 수 없습니다. 또한 이 프로그램 항상 차단 옵션을 선택하여 의심스러운 프로그램 동작에 대한 Real-Time Protection 알림을 통해 프로그램을 차단하도록 응용 프로그램 필터에 추가할 수 있습니다.

차단할 응용 프로그램

응용 프로그램

이 목록에는 구성을 통해 입력하거나 **ProActiv** 구성 요소에 알려 유해한 것으로 분류한 모든 응용 프로그램이 포함됩니다. 목록의 응용 프로그램은 **Avira ProActiv**에 의해 차단되며 컴퓨터 시스템에서 실행할 수 없습니다. 차단된 프로그램이 시작되면 운영 체제 메시지가 나타납니다. 차단할 응용 프로그램은 지정된 경로 및 파일 이름을 기반으로 **Avira ProActiv**에서 식별되며 해당 콘텐츠에 관계없이 차단됩니다.

입력란

차단할 응용 프로그램을 이 상자에 입력합니다. 응용 프로그램을 식별하려면 전체 경로, 파일 이름 및 파일 확장명을 지정해야 합니다. 경로는 응용 프로그램이 있는 드라이브를 표시하거나 환경 변수로 시작해야 합니다.



이 버튼을 클릭하면 표시되는 창에서 차단할 응용 프로그램을 선택할 수 있습니다.

추가

"추가" 버튼을 사용하면 입력란에 지정된 응용 프로그램을 차단할 응용 프로그램 목록으로 전송할 수 있습니다.

참고

운영 체제의 작업에 필요한 응용 프로그램은 추가할 수 없습니다.

삭제

"삭제" 버튼을 사용하면 차단할 응용 프로그램 목록에서 강조 표시된 응용 프로그램을 제거할 수 있습니다.

허용된 응용 프로그램

건너뛰 응용 프로그램 섹션에는 **ProActiv** 구성 요소의 모니터링 대상(신뢰할 수 있는 프로그램으로 분류되며 기본적으로 목록에 포함되어 있는 서명된 프로그램, 신뢰할 수 있는 응용 프로그램으로 분류되어 응용 프로그램 필터에 추가된 모든 응용 프로그램)에서 제외되는 응용 프로그램이 나열됩니다. 허용된 응용 프로그램을 구성에서 이 목록에 추가할 수 있습니다. 또한 **Real-Time Protection** 알림에서 **신뢰할 수 있는 프로그램** 옵션을 사용하여 **Real-Time Protection** 알림을 통해 의심스러운 프로그램 동작에 응용 프로그램을 추가할 수도 있습니다.

건너뛰 응용 프로그램

응용 프로그램

이 목록에는 **ProActiv** 구성 요소의 모니터링 대상에서 제외되는 응용 프로그램이 포함됩니다. 기본 설치 설정에서 목록에는 신뢰할 수 있는 공급자의 서명된 응용 프로그램이 포함됩니다. 사용자가 신뢰할 수 있는 것으로 간주하는 응용 프로그램은 구성이나 **Real-Time Protection** 알림을 통해 추가할 수 있습니다. **ProActiv** 구성 요소는 경로 파일 이름 및 콘텐츠를 사용하여 응용 프로그램을 식별합니다. 업데이트와 같은 변경 사항을 통해 프로그램에 맬웨어가 추가될 수 있으므로 콘텐츠를 검사하는 것이 좋습니다. 지정된 **유형**에서 콘텐츠를 검사할 수행해야 하는지 여부를 결정할 수 있습니다. 예를 들어 "**콘텐츠**" 유형의 경우 **ProActiv** 구성 요소의 모니터링 대상에서 제외하기 전에 경로 및 파일 이름으로 지정된 응용 프로그램에 대해 파일 콘텐츠 변경 내용을 검사합니다. 파일 콘텐츠가 수정된 경우에는 **ProActiv** 구성 요소에서 응용 프로그램을 다시 모니터링합니다. "**경로**" 유형의 경우 **Real-Time Protection**의 모니터링 대상에서 응용 프로그램을 제외하기 전에 콘텐츠 검사가 수행되지 않습니다. 제외 유형을 변경하려면 표시된 유형을 클릭하십시오.

경고

예외적인 경우에만 **경로** 유형을 사용하십시오. 업데이트를 통해 응용 프로그램에 맬코드가 추가될 수 있습니다. 원래 유해한 응용 프로그램은 맬웨어로 분류됩니다.

참고

예를 들면 **Avira** 제품의 모든 응용 프로그램 구성 요소를 포함하여 일부 신뢰할 수 있는 응용 프로그램은 목록에 포함되지 않은 경우에도 기본적으로 **ProActive** 구성 요소의 모니터링 대상에서 제외됩니다.

입력란

이 상자에 **ProActiv** 구성 요소의 모니터링 대상에서 제외할 응용 프로그램을 입력합니다. 응용 프로그램을 식별하려면 전체 경로, 파일 이름 및 파일 확장명을 지정해야 합니다. 경로는 응용 프로그램이 있는 드라이브를 표시하거나 환경 변수로 시작해야 합니다.



이 버튼을 사용하여 표시되는 창에서 제외할 응용 프로그램을 선택할 수 있습니다.

추가

"**추가**" 버튼을 사용하면 입력란에 지정된 응용 프로그램을 제외할 응용 프로그램 목록으로 전송할 수 있습니다.

삭제

"삭제" 버튼을 사용하면 제외할 응용 프로그램 목록에서 강조 표시된 응용 프로그램을 제거할 수 있습니다.

12.10.3 암호

암호를 사용하여 **다양한 영역**에서 Avira 제품을 보호할 수 있습니다. 암호가 지정된 경우 보호된 영역을 열려고 할 때마다 이 암호를 묻는 메시지가 표시됩니다.

암호

암호 입력

여기에 필요한 암호를 입력합니다. 보안을 유지하기 위해 이 공간에 입력하는 실제 문자는 별표(*)로 대체됩니다. 암호의 최대 길이는 **20**자입니다. 암호를 지정한 후에는, 정확하지 않은 암호를 입력할 경우 프로그램에서 액세스가 거부됩니다. 이 상자를 비워 두면 암호가 없음을 의미합니다.

확인

위에서 입력한 암호를 여기에 다시 한 번 입력하여 확인합니다. 보안을 유지하기 위해 이 공간에 입력하는 실제 문자는 별표(*)로 대체됩니다.

참고

암호는 대/소문자를 구분합니다.

암호로 보호된 영역 (옵션은 전문가 모드에서만 사용 가능)

Avira 제품에서는 개별 영역을 암호로 보호할 수 있습니다. 관련 상자를 클릭하여 필요에 따라 개별 영역에 대한 암호 요청을 비활성화하거나 다시 활성화할 수 있습니다.

암호로 보호된 영역	기능
제어 센터	이 옵션을 선택하면 사전 정의된 암호가 있어야 제어 센터를 시작할 수 있습니다.
Real-Time Protection 활성화/비활성화	이 옵션을 선택하면 사전 정의된 암호가 있어야 Avira Real-Time Protection을 사용하거나 사용하지 않도록 설정할 수 있습니다.

<p>Mail Protection 활성화/비활성화</p>	<p>이 옵션을 선택하면 미리 정의된 암호가 있어야 Mail Protection을 사용하거나 사용하지 않도록 설정할 수 있습니다.</p>
<p>FireWall 활성화/비활성화</p>	<p>이 옵션을 선택하면 미리 정의된 암호를 입력해야 FireWall을 활성화하거나 비활성화할 수 있습니다.</p>
<p>Web Protection 활성화/비활성화</p>	<p>이 옵션을 선택하면 미리 정의된 암호를 입력해야 Web Protection을 활성화하거나 비활성화할 수 있습니다.</p>
<p>Safe Browsing 사용/사용 안 함</p>	<p>이 옵션을 선택하면 미리 정의된 암호를 입력해야 자녀 보호를 활성화하거나 비활성화할 수 있습니다.</p>
<p>격리 저장소</p>	<p>이 옵션을 선택하면 암호를 통해 보호되는 격리 관리자의 모든 영역이 활성화됩니다. 관련 상자를 클릭하여 개별 영역에 대해 필요에 따라 암호 사용을 비활성화하거나 다시 활성화할 수 있습니다.</p>
<p>영향받는 개체 복원</p>	<p>이 옵션을 선택하면 미리 정의된 암호를 입력해야 개체를 복원할 수 있습니다.</p>
<p>감염된 개체 다시 검사</p>	<p>이 옵션을 선택하면 미리 정의된 암호를 입력해야 개체를 다시 검사할 수 있습니다.</p>
<p>영향받는 개체 속성</p>	<p>이 옵션을 선택하면 미리 정의된 암호를 입력해야 개체의 속성을 표시할 수 있습니다.</p>
<p>영향받는 개체 삭제</p>	<p>이 옵션을 선택하면 미리 정의된 암호를 입력해야 개체를 삭제할 수 있습니다.</p>
<p>Avira로 전자 메일 보내기</p>	<p>이 옵션을 선택하면 미리 정의된 암호를 입력해야 검사를 위해 Avira 맬웨어 연구 센터로 개체를 보낼 수 있습니다.</p>

영향받는 개체 복사	이 옵션을 선택하면 미리 정의된 암호를 입력해야 영향받는 개체를 복사할 수 있습니다.
작업 추가 및 수정	이 옵션을 선택하면 미리 정의된 암호를 입력해야 스케줄러에서 작업을 추가하고 수정할 수 있습니다.
구성	이 옵션을 선택하면 미리 정의된 암호를 입력해야 프로그램의 구성이 가능합니다.
설치/제거	이 옵션을 선택하면 미리 정의된 암호를 입력해야 프로그램을 설치하거나 제거할 수 있습니다.

12.10.4 보안

고급 모드에서만 사용할 수 있는 옵션입니다.

자동 실행

자동 실행 기능 차단

이 옵션을 선택하면 **USB 스틱, CD 및 DVD 드라이브, 네트워크 드라이브** 등 연결된 모든 드라이브에서 **Windows** 자동 실행 기능의 실행이 차단됩니다. **Windows** 자동 실행 기능을 사용하면 데이터 미디어나 네트워크 드라이브에 있는 파일을 로드 또는 연결되는 즉시 읽으므로 파일을 자동으로 시작하거나 복사할 수 있습니다. 그러나 이 기능에는 자동 시작 시 맬웨어 및 사용자 동의 없이 설치된 프로그램이 설치될 수 있으므로 높은 보안 위험이 따릅니다. 특히 **USB 스틱**의 경우 스틱에 저장된 데이터가 언제든지 변경될 수 있으므로 주의해야 합니다.

CD 및 DVD 제외

이 옵션을 선택하면 **CD 및 DVD 드라이브**에서 자동 실행 기능이 허용됩니다.

경고

신뢰할 수 있는 데이터 미디어를 사용하는 경우에만 **CD 및 DVD 드라이브**에 대해 자동 실행 기능을 해제하십시오.

시스템 보호

Window 호스트 파일 변경 차단

이 옵션을 활성화하면 Windows 호스트 파일이 쓰기 방지됩니다. 따라서 더 이상 수정할 수 없습니다. 예를 들어 맬웨어가 사용자를 원하지 않는 웹 사이트로 리디렉션할 수 없습니다. 이 옵션은 기본 설정으로 활성화됩니다.

제품 보호

참고

사용자 정의 설치 옵션을 사용하여 **Real-Time Protection**을 설치하지 않은 경우에는 제품 보호 옵션을 사용할 수 없습니다.

원치 않게 종료되지 않도록 프로세스 보호

이 옵션을 선택하면 바이러스 및 맬웨어에 의해 사용자 동의 없이 종료되거나 사용자가 작업 관리자 등을 사용하여 '제어되지 않은 상태'로 종료할 수 없도록 프로그램의 모든 프로세스가 보호됩니다. 이 옵션은 기본 설정으로 선택됩니다.

고급 프로세스 보호

이 옵션을 선택하면 프로그램의 모든 프로세스가 사용자 동의 없이 종료될 수 없도록 고급 옵션으로 보호됩니다. 고급 프로세스 보호에는 단순 프로세스 보호보다 훨씬 많은 컴퓨터 리소스가 필요합니다. 이 옵션은 기본적으로 사용하도록 설정됩니다. 이 옵션을 사용하지 않으려면 컴퓨터를 다시 시작해야 합니다.

참고

Windows XP 64비트 암호 보호를 사용할 수 없습니다.

경고

프로세스 보호 기능을 사용하는 경우 다른 소프트웨어 제품과의 상호 작용에 문제가 발생할 수 있습니다. 이러한 경우 프로세스 보호를 해제하십시오.

파일 및 레지스트리 항목을 수정할 수 없도록 보호

이 옵션을 선택하면 프로그램의 모든 레지스트리 항목과 모든 프로그램 파일(이진 파일 및 구성 파일)이 수정할 수 없도록 보호됩니다. 수정할 수 없도록 보호하는 데는 쓰기 및 삭제 보호는 물론 경우에 따라 사용자나 외부 프로그램에 의한 레지스트리 항목 또는 프로그램에 대한 읽기 액세스 보호도 포함됩니다. 이 옵션을 사용하려면 컴퓨터를 다시 시작해야 합니다.

경고

이 옵션을 선택 취소하면 특정 유형 맬웨어에 감염된 컴퓨터의 복구가 실패할 수 있습니다.

참고

이 옵션이 활성화되면 검사 또는 업데이트 요청에 대한 변경 내용을 포함하여 구성만 변경할 수 있으며 사용자 인터페이스를 통해서만 변경할 수 있습니다.

참고

Windows XP 64비트 파일 및 레지스트리 항목 보호를 사용할 수 없습니다.

12.10.5 WMI

고급 모드에서만 사용할 수 있는 옵션입니다

WMI(Windows Management Instrumentation)에 대한 지원

WMI(Windows Management Instrumentation)는 스크립트 및 프로그래밍 언어를 사용하여 Windows 시스템 설정에 로컬 및 원격으로 읽기 및 쓰기 액세스할 수 있도록 해주는 기본 Windows 관리 기술입니다. Avira 제품에서는 WMI를 지원하며 데이터(상태 정보, 통계 데이터, 보고서, 계획된 요청 등)와 이벤트 및 인터페이스를 통해 제공합니다. WMI는 프로그램에서 작동 데이터를 다운로드하고

WMI 지원 사용

이 옵션을 선택하면 WMI를 통해 프로그램에서 작업 데이터를 다운로드할 수 있습니다.

12.10.6 이벤트

고급 모드에서만 사용할 수 있는 옵션입니다.

이벤트 데이터베이스 크기 제한

크기를 최대 n개 항목으로 제한

이 옵션을 사용하면 이벤트 데이터베이스에 나열된 최대 이벤트 수를 특정 크기(예: 100 ~ 10000개 항목)로 제한할 수 있습니다. 입력된 항목 수를 초과하면 가장 오래된 항목이 삭제됩니다.

n일보다 이전인 이벤트 삭제

이 옵션을 사용하면 이벤트 데이터베이스에 나열된 이벤트가 특정 기간(1 ~ 90일)이 지나면 삭제됩니다. 이 옵션은 기본적으로 사용되며 기본값은 30일입니다.

제한 없음

이 옵션을 선택한 경우에는 이벤트 데이터베이스 크기에 제한이 없습니다. 하지만 프로그램 인터페이스의 이벤트 아래에는 최대 20,000개 항목이 표시됩니다.

12.10.7 보고서

고급 모드에서만 사용할 수 있는 옵션입니다.

보고서 제한

최대 수 제한 n개

이 옵션을 선택하면 최대 보고서 수를 특정 수로 제한할 수 있습니다. 1 ~ 300의 값을 사용할 수 있습니다. 지정한 개수를 초과하면 해당 시점에 가장 오래된 보고서가 삭제됩니다.

n일보다 이전인 보고서 모두 삭제

이 옵션을 선택하면 특정 기간(일)이 경과된 경우 보고서가 자동으로 삭제됩니다. 사용할 수 있는 값은 1 ~ 90일입니다. 이 옵션은 기본적으로 사용되며 기본값은 30일입니다.

제한 없음

이 옵션을 선택하면 보고서 수에 대한 제한이 없습니다.

12.10.8 디렉터리

고급 모드에서만 사용할 수 있는 옵션입니다.

임시 경로

기본 시스템 설정 사용

이 옵션을 선택하면, 임시 파일 처리에 시스템의 설정을 사용합니다.

참고

시스템이 임시 파일을 저장하는 위치를 볼 수 있습니다. 예를 들어 Windows XP의 경우에는 시작 > 설정 > 제어판 > 시스템 > 인덱스 카드 "고급" 버튼 "환경

변수"를 누릅니다. 현재 등록된 사용자 및 시스템 변수(TEMP, TMP)에 대한 임시 변수(TEMP, TMP)가 해당 값과 함께 여기에 표시됩니다.

다음 디렉터리 사용

이 옵션을 사용하면 입력란에 표시된 경로가 사용됩니다.

입력란

이 입력란에 프로그램이 임시 파일을 저장하는 경로를 입력합니다.



이 버튼은 필요한 임시 경로를 선택할 수 있는 창을 엽니다.

기본값

이 버튼은 임시 경로에 대해 미리 정의된 디렉터리를 복원합니다.

12.10.9 음향 알림

고급 모드에서만 사용할 수 있는 옵션입니다.

Scanner 또는 **Real-Time Protection**에서 바이러스나 맬웨어가 검색되면 대화형 작업 모드에서 음향 알림이 울립니다. 이제 음향 알림을 활성화하거나 비활성화하도록 선택하고 알림에 사용할 다른 **WAVE** 파일을 선택할 수 있습니다.

참조
Scanner 작업 모드는 [Scanner > 검사 > 검색에 대한 작업](#) 아래의 구성에서 설정합니다. **Real-Time Protection**의 작업 모드는 구성 섹션 [Real-Time Protection > 검사 > 검색에 대한 작업](#)에 있습니다.

경고 없음

이 옵션을 선택하면 **Scanner** 또는 **Real-Time Protection**에서 바이러스가 감지될 때 음향 알림이 울리지 않습니다.

PC 스피커 사용(대화형 모드에서만)

이 옵션을 선택하면 **Scanner** 또는 **Real-Time Protection**에서 바이러스가 감지될 때 기본 신호로 음향 알림이 울립니다. 음향 알림은 PC의 내부 스피커에서 울립니다.

다음 WAVE 파일 사용(대화형 모드에서만)

이 옵션을 선택하면 **Scanner** 또는 **Real-Time Protection**에서 바이러스가 감지될 때 선택된 **WAVE** 파일로 음향 알림을 울립니다. 선택한 **WAVE** 파일은 연결된 외부 스피커를 통해 재생됩니다.

WAVE 파일

이 입력란에 선택한 오디오 파일의 이름과 관련 경로를 입력할 수 있습니다. 프로그램의 기본 음향 신호가 표준으로 입력됩니다.



이 버튼은 파일 탐색기를 사용하여 필요한 파일을 선택할 수 있는 창을 엽니다.

테스트

이 버튼은 선택한 WAVE 파일을 테스트하는 데 사용됩니다.

12.10.10 알림

Avira 제품에서는 특정 이벤트에 대해 성공하거나 실패한 프로그램 시퀀스(예: 업데이트)에 대한 정보를 제공하는 슬라이드 창 형식의 데스크톱 알림을 생성합니다. **알림** 아래에서 특정 이벤트에 대한 알림을 설정하거나 해제할 수 있습니다.

데스크톱 알림을 사용하면 슬라이드 창에서 직접 알림을 해제할 수 있습니다. **알림** 구성 창에서 알림을 비활성화할 수 있습니다.

업데이트

최신 업데이트가 n일보다 이전인 경우 알림

이 상자에는 마지막으로 업데이트한 이후에 업데이트하지 않고 사용할 수 있는 최대 허용 기간(일)을 입력할 수 있습니다. 이 기간(일)이 경과하면 제어 센터의 **상태** 아래에 있는 업데이트 상태에 빨간색 아이콘이 표시됩니다.

바이러스 정의 파일이 만료된 경우 알림 표시

이 옵션을 선택하면 바이러스 정의 파일이 최신 버전이 아닌 경우 알림이 표시됩니다. 이 알림 옵션을 사용하면 마지막 업데이트한 후 n일이 경과된 경우 알림을 표시할 임시 간격을 구성할 수 있습니다.

다음 상황 시 경고/참고

전화 접속 연결 사용

이 옵션을 선택하면 다이얼러에서 전화나 ISDN 네트워크를 통해 컴퓨터에 대한 전화 접속 연결을 생성하는 경우 데스크톱 알림이 제공됩니다. 사용자 동의 없이 설치되는 알 수 없는 다이얼러에 의해 연결이 생성되고 이러한 연결에 대해 요금이 부과될 수 있는 위험이 있습니다. ([바이러스 및 기타 > 위험 범주: 다이얼러 참조](#))

파일 업데이트 성공

이 옵션을 선택하면 업데이트가 성공적으로 수행되고 파일이 업데이트될 때마다 데스크톱 알림이 제공됩니다.

업데이트 실패

이 옵션을 선택하면 업데이트가 실패할 때마다(다운로드 서버에 연결할 수 없거나 업데이트 파일을 설치할 수 없는 경우) 데스크톱 알림이 표시됩니다.

업데이트 필요 없음

이 옵션을 선택하면, 업데이트가 시작되었지만 프로그램이 최신 상태여서 파일을 설치할 필요가 없는 경우 데스크톱 알림이 제공됩니다.

Deze handleiding is met veel zorg gemaakt. Fouten in ontwerp en inhoud zijn echter niet uit te sluiten. Het vermenigvuldigen van deze publicatie in welke vorm dan ook is verboden zonder voorafgaande schriftelijke toestemming van Avira Operations GmbH & Co. KG.

Gepubliceerd 2e kwartaal 2013

Merk- en productnamen zijn handelsmerken of gedeponeerde handelsmerken van hun respectieve eigenaars. Beschermd handelsmerken worden niet als zodanig aangegeven in deze handleiding. Dit betekent echter niet dat deze vrijelijk mogen worden gebruikt.



live free.™